

Steven T. Lovett, OSB No. 910701  
steve.lovett@stoel.com  
Rachel C. Lee, OSB No. 102944  
rachel.lee@stoel.com  
STOEL RIVES LLP  
760 SW Ninth Avenue, Suite 3000  
Portland, OR 97205  
Telephone: 503.224.3380  
Facsimile: 503.220.2480

Daniel F. Katz (*pro hac vice*)  
dkatz@wc.com  
David S. Kurtzer-Ellenbogen (*pro hac vice*)  
dkurtzer@wc.com  
WILLIAMS & CONNOLLY LLP  
725 Twelfth Street, N.W.  
Washington, DC 20005  
Telephone: 202.434.5000  
Facsimile: 202.434.5029

Attorneys for Defendant Intel Corporation

UNITED STATES DISTRICT COURT  
DISTRICT OF OREGON  
PORTLAND DIVISION

In re INTEL CORP. CPU MARKETING,  
SALES PRACTICES AND PRODUCTS  
LIABILITY LITIGATION

Case No.: 3:18-md-2828-SI

---

This Document Relates to All Actions

DEFENDANT INTEL CORPORATION'S  
MOTION TO DISMISS THE AMENDED  
COMPLAINT PURSUANT TO FED. R.  
CIV. P. 9(b), 12(b)(1), AND 12(b)(6)

*Oral Argument Requested*

---

## **TABLE OF CONTENTS**

TABLE OF AUTHORITIES .....	iii
LR 7-1 CERTIFICATION .....	1
MOTION.....	1
LEGAL MEMORANDUM .....	1
INTRODUCTION .....	1
FACTS .....	5
A.    Performance and Security in Modern CPUs.....	5
B.    The Breakthrough Discovery of Speculative-Execution-Based Vulnerabilities.....	6
C.    Intel’s Response to the Novel Vulnerabilities. ....	8
D.    Intel’s Marketing Statements. ....	9
E.    The Named Plaintiffs. ....	9
F.    The Factual Allegations Here Are Materially Indistinguishable from <i>Hauck</i> . ....	10
STANDARD OF REVIEW .....	12
ARGUMENT.....	13
I.    PLAINTIFFS FAIL TO STATE A FRAUD CLAIM UNDER CALIFORNIA LAW (COUNTS I-IV).....	13
A.    Plaintiffs Allege No Actionable Omissions.....	14
1.    Plaintiffs Fail To Satisfy Rule 9(b) as to the Nature of Any Defect.....	14
2.    Plaintiffs Do Not Allege a Central Functional Defect. ....	16
3.    Plaintiffs’ Omission Claims Also Fail Because They Identify No Duty To Disclose Under the <i>LiMandri</i> Factors. ....	17
4.    Plaintiffs Fail To Plead that Intel’s Alleged Omissions Were Material to Reasonable Consumers. ....	21
B.    Plaintiffs Fail To State a Claim Based on Affirmative Misrepresentations.....	24

1.	No Plaintiff Alleges Viewing Any Specific Misrepresentation.....	24
2.	<i>Hauck</i> 's Reasoning Forecloses Plaintiffs' Affirmative Misrepresentation Claim as a Matter of Law.....	26
C.	Plaintiffs Cannot Pursue Equitable Remedies Under the California Statutes.....	28
II.	PLAINTIFFS FAIL TO STATE A CLAIM FOR UNFAIR OR UNLAWFUL TRADE PRACTICES UNDER CALIFORNIA LAW (COUNT III). ....	30
A.	Plaintiffs Do Not Plead Any Unfair Trade Practice.....	30
1.	<i>Hauck</i> Supports Dismissal of Plaintiffs' Unfair-Practices Claim.....	31
2.	California Law Bars Plaintiffs' "Unfair Design Choice" Theory.....	33
B.	Plaintiffs Do Not Plead Any Unlawful Trade Practice.....	35
III.	PLAINTIFFS FAIL TO STATE A CLAIM FOR UNJUST ENRICHMENT OR QUASI-CONTRACT UNDER CALIFORNIA LAW (COUNT V). ....	35
IV.	PLAINTIFFS FAIL TO STATE A CLAIM FOR ANY BELLWETHER COUNT. ....	37
A.	Plaintiffs State No Bellwether Claim for Omissions. ....	37
B.	Plaintiffs State No Bellwether Claim for Affirmative Misrepresentations.....	41
C.	Plaintiffs State No Bellwether Claim for "Unfair" Trade Practices. ....	43
D.	Plaintiffs State No Bellwether Claim for "Unconscionable" Conduct. ....	44
E.	No Bellwether Claim Can Advance Without a Named Plaintiff. ....	47
	CONCLUSION.....	47

## **TABLE OF AUTHORITIES**

### **FEDERAL CASES**

<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009) .....	12, 45
<i>Astiana v. Hain Celestial Group</i> , 783 F.3d 753 (9th Cir. 2015) .....	36
<i>Barrett-O’Neill v. Lalo, LLC</i> , 171 F. Supp. 3d 725 (S.D. Ohio 2016) .....	45
<i>Batson v. Live Nation Entertainment, Inc.</i> , 746 F.3d 827 (7th Cir. 2014) .....	43, 44
<i>Bell Atlantic Corp. v. Twombly</i> , 550 U.S. 544 (2007) .....	12
<i>Bober v. Glaxo Wellcome PLC</i> , 246 F.3d 934 (7th Cir. 2001) .....	42
<i>Coffey v. WCW &amp; Air, Inc.</i> , 2020 WL 3250744 (N.D. Fla. Mar. 25, 2020) .....	44, 45
<i>Davis v. HSBC Bank</i> , 691 F.3d 1152 (9th Cir. 2012) .....	30
<i>Deburro v. Apple, Inc.</i> , 2013 WL 5917665 (W.D. Tex. Oct. 31, 2013) .....	41, 42
<i>Ebner v. Fresh, Inc.</i> , 838 F.3d 958 (9th Cir. 2016) .....	27
<i>Elias v. Hewlett-Packard Co.</i> , 903 F. Supp. 2d 843 (N.D. Cal. 2012) .....	13, 14, 30
<i>Fink v. Time Warner Cable</i> , 714 F.3d 739 (2d Cir. 2013) (per curiam) .....	42
<i>Garcia v. Sony Computer Entertainment America, LLC</i> , 859 F. Supp. 2d 1056 (N.D. Cal. 2012) .....	25, 26, 28
<i>Great Pacific Securities v. Barclays Capital, Inc.</i> , 743 F. App’x 780 (9th Cir. 2018) .....	26
<i>Guaranty Trust Co. v. York</i> , 326 U.S. 99 (1945) .....	29
<i>Hall v. Sea World Entertainment, Inc.</i> , 2015 WL 9659911 (S.D. Cal. Dec. 23, 2015) .....	41
<i>Halperin v. International Web Services, LLC</i> , 123 F. Supp. 3d 999 (N.D. Ill. 2015) .....	43
<i>Hauck v. Advanced Micro Devices, Inc.</i> , --- F. App’x ---, 2020 WL 2510754 (9th Cir. May 15, 2020) .....	<i>passim</i>
<i>Hauck v. Advanced Micro Devices, Inc.</i> , 2019 WL 1493356 (N.D. Cal. Apr. 4, 2019) ....	17, 31, 38
<i>Henryhand v. Dorel Juvenile Group</i> , 2017 WL 7806590 (C.D. Cal. Oct. 5, 2017) .....	33
<i>Hodsdon v. Mars, Inc.</i> , 891 F.3d 857 (9th Cir. 2018) .....	16, 17, 21, 31
<i>Hovsepian v. Apple Inc.</i> , 2009 WL 5069144 (N.D. Cal. Dec. 17, 2009) .....	21, 22, 37

<i>Ibarrola v. Kind, LLC</i> , 83 F. Supp. 3d 751 (N.D. Ill. 2015).....	42
<i>In re Apple Inc. Device Performance Litigation</i> , 347 F. Supp. 3d 434 (N.D. Cal. 2018).....	28, 30, 31, 34
<i>In re General Motors LLC Ignition Switch Litigation</i> , 257 F. Supp. 3d 372 (S.D.N.Y. 2017).....	40
<i>In re Intel Corp. Securities Litigation</i> , 2019 WL 1427660 (N.D. Cal. Mar. 29, 2019).....	27
<i>In re NVIDIA Corp. Securities Litigation</i> , 768 F.3d 1046 (9th Cir. 2014).....	13
<i>In re Sling Media Slingbox Advertising Litigation</i> , 202 F. Supp. 3d 352 (S.D.N.Y. 2016) .....	39
<i>Jaramillo v. Liberty Mutual Insurance Co.</i> , 2019 WL 8223608 (N.D. Tex. Apr. 29, 2019).....	46
<i>Karpowicz v. General Motors Corp.</i> , 1997 WL 413929 (N.D. Ill. July 18, 1997).....	38
<i>Kearns v. Ford Motor Co.</i> , 567 F.3d 1120 (9th Cir. 2009) .....	25, 26, 41
<i>Khoja v. Orexigen Therapeutics, Inc.</i> , 899 F.3d 988 (9th Cir. 2018) .....	13
<i>Kondash v. Kia Motors America, Inc.</i> , 2016 WL 11246421 (S.D. Ohio June 24, 2016) .....	39
<i>Marlowe v. Nature’s Bounty Co.</i> , 2017 WL 2291683 (N.D. Ohio May 25, 2017) .....	41
<i>Matthews v. American Honda Motor Co.</i> , 2012 WL 2520675 (S.D. Fla. June 6, 2012).....	39
<i>Mazza v. American Honda Motor Co.</i> , 666 F.3d 581 (9th Cir. 2012) .....	13
<i>Moss v. U.S. Secret Service</i> , 572 F.3d 962 (9th Cir. 2009).....	12
<i>Myers v. BMW of North America, LLC</i> , 2016 WL 5897740 (N.D. Cal. Oct. 11, 2016) .....	14
<i>Noll v. eBay Inc.</i> , 2013 WL 2384250 (N.D. Cal. May 30, 2013) .....	23
<i>O’Shea v. Littleton</i> , 414 U.S. 488 (1974) .....	29
<i>Pardini v. Unilever U.S., Inc.</i> , 961 F. Supp. 2d 1048 (N.D. Cal. 2013) .....	47
<i>Popejoy v. Sharp Electronics Corp.</i> , 2015 WL 5545067 (D.N.J. Sept. 18, 2015) .....	42
<i>Punian v. Gillette Co.</i> , 2016 WL 1029607 (N.D. Cal. Mar. 15, 2016).....	22
<i>Rogers v. Cisco Systems, Inc.</i> , 268 F. Supp. 2d 1305 (N.D. Fla. 2003).....	45
<i>Rojas-Lozano v. Google, Inc.</i> , 159 F. Supp. 3d 1101 (N.D. Cal. 2016) .....	13

<i>Rosenthal v. Sharkninja Operating LLC</i> , 2016 WL 7338535 (D.N.J. Dec. 19, 2016) .....	41
<i>Slebochnik v. Reynolds &amp; Reynolds Co.</i> , 2014 WL 6609132 (D.N.J. Nov. 20, 2014) .....	45
<i>Smajlaj v. Campbell Soup Co.</i> , 782 F. Supp. 2d 84 (D.N.J. 2011) .....	38
<i>Sonner v. Premier Nutrition Corp.</i> , 962 F.3d 1072 (9th Cir. 2020) .....	28, 29, 36
<i>Sud v. Costco Wholesale Corp.</i> , 229 F. Supp. 3d 1075 (N.D. Cal. 2017) .....	24
<i>Szymczak v. Nissan North America Inc.</i> , 2011 WL 7095432 (S.D.N.Y. Dec. 16, 2011) .....	41
<i>Tabler v. Panera LLC</i> , 2020 WL 3544988 (N.D. Cal. June 30, 2020) .....	25
<i>Vess v. Ciba-Geigy Corp. USA</i> , 317 F.3d 1097 (9th Cir. 2003) .....	14
<i>Ward v. Bolek</i> , 2013 WL 145828 (D. Or. Jan. 14, 2013) .....	12
<i>Wilson v. Hewlett-Packard Co.</i> , 668 F.3d 1136 (9th Cir. 2012) .....	18, 19
<i>Woods v. Maytag Co.</i> , 2010 WL 4314313 (E.D.N.Y. Nov. 2, 2010) .....	41
<i>Yastrab v. Apple, Inc.</i> , 173 F. Supp. 3d 972 (N.D. Cal. 2016) .....	27, 28
<i>Zucco Partners, LLC v. Digimarc Corp.</i> , 552 F.3d 981 (9th Cir. 2009) .....	13

## STATE CASES

<i>Bardin v. DaimlerChrysler Corp.</i> , 39 Cal. Rptr. 3d 634 (Ct. App. 2006) .....	<i>passim</i>
<i>Chastain v. Koonce</i> , 700 S.W.2d 579 (Tex. 1985) .....	46
<i>D'Agostino v. Maldonado</i> , 78 A.3d 527 (N.J. 2013) .....	45
<i>De Bouse v. Bayer AG</i> , 922 N.E.2d 309 (Ill. 2009) .....	40, 41
<i>Frank v. DaimlerChrysler Corp.</i> , 741 N.Y.S.2d 9 (App. Div. 2002) .....	40
<i>Ghirardo v. Antonioli</i> , 924 P.2d 996 (Cal. 1996) .....	36
<i>Gomez-Jimenez v. New York Law School</i> , 956 N.Y.S.2d 54 (App. Div. 2012) .....	38
<i>Grgat v. Giant Eagle, Inc.</i> , 135 N.E.3d 846 (Ohio Ct. App. 2019) .....	38, 42
<i>Hartford Casualty Insurance Co. v. J.R. Marketing, LLC</i> , 353 P.3d 319 (Cal. 2015) .....	36
<i>Himelsein Mandel Fund Management, LLC v. Fortress Investment Group</i> , 2019 WL 1395963 (Cal. Ct. App. Mar. 28, 2019) .....	36
<i>Johnson v. Microsoft Corp.</i> , 834 N.E.2d 791 (Ohio 2005) .....	45

<i>Judge v. Blackfin Yacht Corp.</i> , 815 A.2d 537 (N.J. Super. Ct. App. Div. 2003).....	39
<i>LiMandri v. Judkins</i> , 60 Cal. Rptr. 2d 539 (Ct. App. 1997) .....	<i>passim</i>
<i>Nationwide Biweekly Administration, Inc. v. Superior Court</i> , 462 P.3d 461 (Cal. 2020) .....	29
<i>Oswego Laborers’ Local 214 Pension Fund v. Marine Midland Bank, N.A.</i> , 647 N.E.2d 741 (N.Y. 1995).....	38, 42
<i>Otworth v. Southern Pacific Transportation Co.</i> , 212 Cal. Rptr. 743 (Ct. App. 1985).....	36
<i>PNR, Inc. v. Beacon Property Management</i> , 842 So. 2d 773 (Fla. 2003) .....	38, 42, 43
<i>Porsche Cars North America, Inc. v. Diamond</i> , 140 So. 3d 1090 (Fla. Dist. Ct. App. 2014) .....	43
<i>Prakashpalan v. Engstrom, Lipscomb &amp; Lack</i> , 167 Cal. Rptr. 3d 832 (Ct. App. 2014) .....	36
<i>Professional Tax Appeal v. Kennedy-Wilson Holdings, Inc.</i> , 239 Cal. Rptr. 3d 908 (Ct. App. 2018) .....	36
<i>Rockford Memorial Hospital v. Havrilesko</i> , 858 N.E.2d 56 (Ill. App. Ct. 2006).....	39
<i>Seely v. White Motor Co.</i> , 403 P.2d 145 (Cal. 1965).....	33
<i>Trejo v. Johnson &amp; Johnson</i> , 220 Cal. Rptr. 3d 127 (Ct. App. 2017) .....	34
<i>Washburn v. Sterling McCall Ford</i> , 521 S.W.3d 871 (Tex. App. 2017).....	39
<i>Yalley v. Liberty Life Assurance Co.</i> , 2019 WL 2710242 (Cal. Ct. App. June 28, 2019) .....	36

## STATUTES AND RULES

California Consumers Legal Remedies Act, Cal. Civ. Code § 1770.....	<i>passim</i>
California False Advertising Law, Cal. Bus. & Prof. Code § 17500.....	<i>passim</i>
California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200.....	<i>passim</i>
Federal Rule of Civil Procedure 9(b).....	<i>passim</i>
Federal Rule of Civil Procedure 12(b)(1) .....	1
Federal Rule of Civil Procedure 12(b)(6) .....	1, 12, 28, 30
Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. § 501.201 <i>et seq.</i> .....	<i>passim</i>
Illinois Consumer Fraud and Deceptive Business Practices Act, 815 Ill. Comp. Stat. 505 ..	<i>passim</i>

New Jersey Consumer Fraud Act, N.J. Stat. Ann. § 56:8-1 <i>et seq.</i> .....	<i>passim</i>
New York General Business Law, N.Y. Gen. Bus. Law § 349 <i>et seq.</i> .....	<i>passim</i>
Ohio Consumer Sales Practices Act, Ohio Rev. Code § 1345.01 <i>et seq.</i> .....	<i>passim</i>
Texas Deceptive Trade Practices Act, Tex. Bus. & Com. Code § 17.41 <i>et seq.</i> .....	<i>passim</i>



### **LR 7-1 CERTIFICATION**

Pursuant to LR 7-1(a), undersigned counsel certifies that the parties discussed this motion in good faith via telephone conference on July 27, 2020, and were unable to reach a resolution.

### **MOTION**

Defendant Intel Corporation respectfully moves the Court to dismiss with prejudice all California law counts (Counts I-V, for fraud by concealment and omission, for violations of the Consumers Legal Remedies Act (“CLRA”), Unfair Competition Law (“UCL”), and False Advertising Law (“FAL”), and for quasi-contract or unjust enrichment) of the Amended Consolidated Class Action Allegation Complaint (“Amended Complaint” or “AC”), ECF No. 181, and all six bellwether claims (under the laws of Florida, Illinois, New Jersey, New York, Ohio, and Texas, as identified *infra* Section IV) pursuant to Federal Rules of Civil Procedure 9(b), 12(b)(1), and 12(b)(6). All of these counts fail to state a claim upon which relief can be granted, and Plaintiffs lack standing to bring claims under the law of a state where no named Plaintiff resides. Oral argument is requested.

### **LEGAL MEMORANDUM**

#### **INTRODUCTION**

Since the Court decided Intel’s motion to dismiss the prior Complaint, the Ninth Circuit has spoken clearly on the issues in this case. *See Hauck v. Advanced Micro Devices, Inc.*, --- F. App’x ---, 2020 WL 2510754 (9th Cir. May 15, 2020). In affirming dismissal with prejudice upon *de novo* review, the *Hauck* panel concluded that the design features of AMD’s processors and AMD’s conduct regarding Spectre were neither deceptive nor unfair as a matter of law. In particular, the Ninth Circuit rejected the *Hauck* plaintiffs’ claim that AMD defrauded them by not disclosing vulnerabilities based on “side channel attacks generally” or because of “some . . . subset of their [processors’] features” independent of a specific vulnerability such as

“Spectre-like attacks in particular.” *See id.* at \*2. The court further held that reasonable consumers do not expect their devices to be “completely impervious to novel cybersecurity threats” and that the plaintiffs could not state a claim based on “the theoretical risk of a cybersecurity flaw that has not yet been successfully exploited.” *See id.*<sup>1</sup>

Every claim in the Amended Complaint here fails for the reasons set forth in *Hauck*. Both cases involve allegations that Intel and AMD knew that certain performance-enhancing features in their processors’ designs carried a “theoretical risk of a cybersecurity flaw that has not yet been successfully exploited.” *Id.* But those design features existed for more than a decade before a researcher discovered a novel way to manipulate them under lab conditions, yielding the first of the vulnerabilities at issue here. Neither set of plaintiffs can explain how the 2017 discovery of specific vulnerabilities in their devices, which all parties agree were unknown to the manufacturer at the time of sale, could have deprived them of any reasonably expected bargain. And even now, nearly three years after the public disclosure of Spectre and Meltdown, Plaintiffs still cannot allege that any of them, or anyone else, has suffered a real-world data breach.

Plaintiffs’ principal theory is that Intel fraudulently concealed “defects” in its processor design. That theory fails outright because of a fundamental timing problem Plaintiffs cannot avoid—the design features they identify long predate any vulnerability at issue here. It also fails as to Plaintiffs’ California common law, CLRA, and UCL claims because Plaintiffs can identify no central functional defect, nor can they satisfy any of the *LiMandri* factors. In fact, millions of consumers (and nearly all Named Plaintiffs) are still using their Intel-based devices, and *Hauck*

---

<sup>1</sup> Although *Hauck* is unpublished, it is persuasive authority from a Ninth Circuit panel. *Hauck* is especially persuasive because it is not cited for a related point of law in an otherwise unrelated case, but rather deals with virtually identical substantive facts and issues as this case.

held that AMD’s processors were fit for ordinary use despite allegations that the plaintiffs in that case experienced slowdowns and “crashes” and that some no longer used their devices. 2020 WL 2510754, at \*3; Ex. 1 (*Hauck* Compl.) ¶¶ 170, 171.<sup>2</sup> Plaintiffs’ tacit recognition that Intel processors are fit for use means there is no central functional defect. Plaintiffs also cannot allege Intel’s pre-sale knowledge of a defect under *LiMandri*. By alleging only Intel’s pre-sale knowledge of “some . . . subset of [its processors’] features,” rather than a specific vulnerability, Plaintiffs fail to allege any actionable fraud. *Hauck*, 2020 WL 2510754, at \*2. Nor can Plaintiffs skirt this result by alleging that Intel’s processors include a second design feature not present in AMD’s processors. Plaintiffs’ fundamental approach here is the same as in *Hauck*: they contend that when researchers discover a novel security vulnerability, the performance-enhancing design features that the vulnerability manipulates should be retrospectively labeled “defects.” As in *Hauck*, that approach should fail.

Plaintiffs’ next theory—that Intel affirmatively misrepresented the speed and security of its processors, or stated half-truths—is equally deficient. As *Hauck* recognized, Plaintiffs’ purported expectations of perfect security (devices “free from potential exploits,” *e.g.*, AC ¶ 41) are unreasonable as a matter of law, and representations about performance do not carry implicit security promises. Plaintiffs thus would fail to state a claim for any affirmative misrepresentation on this ground alone—including under the CLRA, UCL, or FAL—even if any Named Plaintiff could allege seeing a specific Intel security or performance representation, which none does.

---

<sup>2</sup> The operative complaint that the Ninth Circuit reviewed *de novo* in *Hauck*, Am. Consol. Class Action Compl., *Hauck v. Advanced Micro Devices, Inc.*, No. 5:18-cv-00447-LHK (N.D. Cal. filed Dec. 6, 2018), ECF No. 95, is attached to the Declaration of Steven Lovett (“Lovett Decl.”) as Exhibit 1 for the convenience of the Court.

Plaintiffs also allege that Intel committed “unfair” business practices by trading security for speed in its processor design. But the *Hauck* plaintiffs made that same claim, and the Ninth Circuit found it implausible as a matter of law to allege “that the harm represented by the theoretical risk of a cybersecurity flaw that has not yet been successfully exploited outweighs the other benefits of AMD’s processor design.” 2020 WL 2510754, at \*2. Here, Plaintiffs reinforce that holding by emphasizing that consumers “*really* care about” processor speed and that “milliseconds matter.” AC ¶¶ 683, 687 (emphasis in original).<sup>3</sup> Plaintiffs’ premise is that Intel implemented design features to make processors faster, which is critically important to users, and in order to get that significant benefit, created a *theoretical* risk. But California law recognizes that design tradeoffs like these, which are inevitable in developing complex products, cannot give rise to a claim for unfair business practices in the absence of a breach of warranty or physical safety risk, neither of which is alleged here.

Plaintiffs’ reasonable expectations were not violated. Their devices remain fit for use. They can identify no misrepresentation. And they can allege no pre-sale knowledge by Intel of any actual defect in its processors. As such, Plaintiffs cannot state any supposed “nationwide” cause of action under California law, including for unjust enrichment, which requires some underlying wrongdoing. Their claims under the six putative state subclass claims that the parties agreed to brief for purposes of this Motion fail for many of the same reasons (as well as the absence of any Ohio Named Plaintiff at all). *See* Pretrial Order No. 8, ECF No. 186. The Court should dismiss with prejudice all of the California-law counts and all six bellwether counts.

---

<sup>3</sup> All emphasis is added unless otherwise stated.

## FACTS<sup>4</sup>

### A. Performance and Security in Modern CPUs.

Modern CPUs rely on various design strategies to provide the performance expected by contemporary users. One such strategy, incorporated in essentially all modern CPUs, is the use of “out-of-order execution” and “speculative execution.” AC ¶¶ 442-53. The CPU receives program instructions in the order in which the program requests the CPU to perform them. AC ¶ 442. Out-of-order execution lets the CPU compute instructions in a different order from what the program sent rather than, for example, pausing the whole program to wait for data from a distant memory location. AC ¶¶ 442-49. Speculative execution allows the CPU to make an educated guess as to which path a program will take and then execute instructions along that path, discarding unnecessary results. AC ¶¶ 450-53. Out-of-order execution and speculative execution are foundational design features of modern processors from all manufacturers. *See* AC ¶ 455.

Modern CPUs also rely on resource sharing—like shared memory caches or other CPU components—to deliver improved performance to users. *See, e.g.*, AC ¶¶ 18, 471, 479, 483. Sharing resources in this manner allows the CPU “to balance power, efficiency, and thermal output.” AC ¶ 483. Without shared resources, a computer could not run multiple applications at the same time, let alone achieve the performance modern users expect. *See, e.g.*, AC ¶ 683 (“Users *really* care about speed in interactive environments.”) (emphasis in original); AC ¶ 687 (“When talking about responsiveness to performance requests, *milliseconds* matter.”).

---

<sup>4</sup> The facts in the Amended Complaint are assumed true for purposes of this motion only. All exhibits referenced are attached to the Lovett Declaration.

Resource sharing carries intrinsic risk. As Plaintiffs themselves acknowledge, “any time a resource is shared, there is a possibility information can leak.” AC ¶ 520. The discovery of security vulnerabilities within the design of computing products—including CPUs of every manufacturer—is accordingly routine, and computer purchasers expect it. *See Hauck*, 2020 WL 2510754, at \*2-3. Such vulnerabilities are so common that the industry has created “a standardized, industry-endorsed list of security vulnerabilities” called “Common Vulnerabilities and Exposures” or “CVE,” which identifies each vulnerability with a unique number. AC ¶ 21 n.9. “Due to the ever increasing volume of public vulnerability reports,” the CVE numbering system was revamped in 2014 to “track more than 10,000 [new] vulnerabilities in a single year.” Ex. 2 (Mitre, CVE Frequently Asked Questions (cited in AC ¶ 576 n.87)) at 7-8.

**B. The Breakthrough Discovery of Speculative-Execution-Based Vulnerabilities.**

Speculative execution, out-of-order execution, cache memory, and resource sharing were “considered for decades to be harmless and valuable performance features.”<sup>5</sup> In mid-2017, however, a Google engineer made a ground-breaking discovery and drafted a “proof of concept” for the first of what has become a brand-new class of “side-channel” vulnerabilities that leverage these ubiquitous features.<sup>6</sup> This first vulnerability was later named “Spectre.” AC ¶ 613. Based on the articles cited in Plaintiffs’ Amended Complaint, the extraordinary insight behind these specific vulnerabilities was an “innovative use of speculative execution”<sup>7</sup> as the basis for “an

---

<sup>5</sup> Ex. 3 (Claudio Canella et al., *Fallout: Leaking Data on Meltdown-resistant CPUs* (CCS ’19 Proceedings (Nov. 2019)) (cited in AC ¶ 581)) at 1.

<sup>6</sup> Side channels are vulnerabilities based on observation of (sometimes minute) physical differences. For example, any time a processor does one thing faster than another (or generates more heat doing one thing than another, or makes a different sound, etc.), an observer may be able to infer what the processor is doing.

<sup>7</sup> Ex. 4 (*Decyphering the Noise Around ‘Meltdown’ and ‘Spectre’*, McAfee (Jan. 4, 2018) (cited in AC ¶ 636)).

entirely new class of fault-driven transient-execution attacks.”<sup>8</sup> Subsequent variants of this novel class of vulnerabilities include “Meltdown,” “Foreshadow,” “MDS,” and “SWAPGS.” AC ¶¶ 542, 554, 569, 575. These vulnerabilities all operate in fundamentally the same way, as Plaintiffs acknowledge, leveraging aspects of CPU design “related to memory access protection and speculative execution of computer program instructions.” AC ¶ 5.

Plaintiffs expressly concede that Intel learned of this new class of vulnerabilities for the first time in June of 2017. AC ¶ 613. Plaintiffs cite academic papers published as early as 2006 that *theorize* about the *possibility* of certain types of security vulnerabilities in the CPUs of Intel and other manufacturers, but they do not allege that any of these earlier publications actually disclosed Spectre, Meltdown, or any other member of the new class of specific vulnerabilities discovered in 2017. This new class of speculative execution vulnerabilities affects all CPU manufacturers in some form. *See, e.g.*, AC ¶¶ 621, 638 (alleging AMD is vulnerable to Spectre). Plaintiffs’ own authorities also make clear that AMD processors are, in turn, subject to security vulnerabilities that do not affect Intel, such as “the Ryzenfall bugs [that] would have allowed attackers to take full control of the AMD Secure Processor.”<sup>9</sup>

Recognizing that Intel cannot fail to disclose vulnerabilities of which it was not aware, Plaintiffs attempt to turn back the clock. They describe two features of Intel’s CPU design—which they label “Unauthorized Access” and “Incomplete Undo”—that they now say constituted

---

<sup>8</sup> Ex. 5 (Michael Schwarz et al., *ZombieLoad: Cross-Privilege-Boundary Data Sampling* (2019) (cited in AC ¶ 575)).

<sup>9</sup> Ex. 6 (Lucian Armasu, *Intel vs AMD Processor Security: Who Makes the Safest CPUs?*, Tom’s Hardware (Nov. 4, 2019) (cited in AC ¶ 641)) at 5-6. These AMD vulnerabilities “have a very high severity rating.” *Id.* In March 2020, AMD itself disclosed a speculative execution-based side channel variant, “Take A Way,” to which *Intel* CPUs are not susceptible. AMD Product Security, *Take A Way* (Mar. 7, 2020), <https://www.amd.com/en/corporate/product-security> (new variant permits unauthorized user to “transmit user data in an unintended way”).

“defects” for many years. AC ¶¶ 5-8.<sup>10</sup> They claim these “defects” are independent of the vulnerabilities discovered in 2017 and later. AC ¶ 5. Thus, Plaintiffs contend, an Intel CPU purchased in 2006, eleven years before the discovery of Spectre and Meltdown, was nonetheless “defective” from the moment of purchase, even though it worked exactly as promised and the design features at issue had no known vulnerabilities.

Plaintiffs also now claim that the vulnerabilities have been “weaponized,” in that proof-of-concept code is available on the internet. AC ¶¶ 631-34. That sounds scary, but Plaintiffs’ citations on that point date back to January or February 2018, immediately after Spectre and Meltdown were disclosed, and seven months before the *prior* consolidated complaint was filed. *Id.* There is nothing new here. Despite Plaintiffs’ allegation that proof-of-concept code has been available for almost three years, Plaintiffs do not allege that any person has ever had any data stolen through any of these vulnerabilities.

### **C. Intel’s Response to the Novel Vulnerabilities.**

When Intel and other CPU manufacturers first learned of this new class of vulnerabilities in 2017, they worked to develop mitigations (or “patches”) that can be deployed remotely to address security issues post-manufacture. AC ¶¶ 656, 698. Plaintiffs allege that these mitigations cumulatively reduce the performance of their CPUs to the performance of an earlier generation processor (tacitly acknowledging that those mitigations plainly do not render the

---

<sup>10</sup> Plaintiffs define Unauthorized Access as the CPU “creat[ing] windows of time during which an unauthorized user could have the processor make unnecessary or unauthorized memory accesses to copies of sensitive or privileged information.” AC ¶ 507. They define Incomplete Undo as the CPU “allow[ing] that information (or critical data about the location or contours of that information) to remain in the CPUs’ caches after the mistaken or unauthorized access (e.g., an exception) was discovered.” *Id.*



device inoperable), but also recognize that “how much the system is impacted depends on the characteristics of the application being tested.” AC ¶¶ 679, 759-60.

#### **D. Intel’s Marketing Statements.**

Plaintiffs note advertisements stating, for example, that Intel CPUs are “secure” or “secure to the core.” AC ¶¶ 499-502. No such advertisement represented that an Intel CPU would be impervious to all *future, undiscovered* security vulnerabilities. Plaintiffs also note certain of Intel’s performance-related advertisements. *See, e.g.*, AC ¶¶ 689-90. But none of those performance advertisements guaranteed any particular level of security, whether explicitly or implicitly, or that the precise performance levels at the time of sale would be sustained through all future patches.

#### **E. The Named Plaintiffs.**

The Amended Complaint consolidates the claims of 45 Named Plaintiffs (down from 95, *see* ECF No. 115).<sup>11</sup> The six bellwether states and California have ten Named Plaintiffs in total, but there is no Named Plaintiff for Ohio.<sup>12</sup>

Each of these individual Named Plaintiffs alleges having bought devices containing Intel processors from third parties, such as Amazon or Best Buy. *E.g.*, AC ¶¶ 41, 108. They formulaically recite that when they purchased their devices, they “reviewed and relied on the information about the [computer] and Intel processor that was displayed [in the store or online].” *E.g.*, AC ¶¶ 292, 298. None alleges the content of this information with any

---

<sup>11</sup> The Amended Complaint no longer names the five Named Plaintiffs who purchased devices after the January 2018 public disclosure of Spectre and Meltdown. *See* ECF No. 115, ¶¶ 15, 22, 24, 82, 111. But it retains all five as putative class members, along with millions of others who bought devices with Intel CPUs from January 2018 to the present. AC ¶ 780.

<sup>12</sup> There is also no Named Plaintiff for 19 other states for which Plaintiffs purport to bring subclass claims.

particularity—none identifies any specific claim or representation relied upon. Yet each alleges that had Intel disclosed the alleged “Defects in the Intel CPUs, or that mitigations needed to address the Defects would materially impact the CPUs’ functionality and performance,” they “would have seen [such disclosures] and no doubt have taken them into account in making [their] purchasing decision.” *E.g.*, AC ¶¶ 198, 353. The entity Named Plaintiff from Florida does not allege where it purchased its devices, nor what, if any, advertisements it saw concerning Intel processors, but nonetheless alleges that had the “defects” or mitigations needed to address them been displayed in Intel advertisements, it “would have seen them and no doubt have taken them into account in making its purchasing decisions.” AC ¶ 78.

No Named Plaintiff alleges experiencing any hack or data breach. The Named Plaintiffs allege “reduced processing speed” (which they support not through any analysis of their own devices, but only via supposedly comparable “test machines”), and allege other issues like “freezing” or “unexpected shutdowns.” *E.g.*, AC ¶¶ 43-44, 116-17. Despite these asserted difficulties, all Named Plaintiffs from the six bellwether states and California continue to use their Intel CPUs. *See* AC ¶¶ 42, 48, 75, 109, 115, 194, 206, 293, 299, 349.

**F. The Factual Allegations Here Are Materially Indistinguishable from *Hauck*.**

The allegations in *Hauck*, which the Ninth Circuit reviewed *de novo* and agreed failed to state a claim, are functionally identical to the allegations here. While Plaintiffs here allege that Intel CPUs are subject to vulnerability variants (such as Meltdown) to which AMD processors are not susceptible, AC ¶ 638, they do not allege facts showing why that distinction makes a legal difference. The striking similarities include the following:

- Plaintiffs allege that the novel vulnerabilities allow unauthorized access to protected data. *See* AC ¶ 1. So did the *Hauck* plaintiffs. Ex. 1 (*Hauck* Compl.) ¶ 66 (“[T]he design of AMD’s CPU microarchitecture created security vulnerabilities that could be easily exploited by attackers, jeopardizing the confidentiality of consumers’ sensitive information.”).

- Plaintiffs try to overcome the recency and novelty of the vulnerabilities by alleging “defects” of which Intel was purportedly previously aware, because Intel knows its own designs. *See* AC ¶¶ 5-6, 507. So did the *Hauck* plaintiffs as to AMD. *See* Ex. 1, ¶¶ 113-15 (describing underlying defect in AMD’s design, allegedly distinct from Spectre).
- Plaintiffs allege that Intel concealed the “defects.” *See* AC ¶¶ 14, 531. So did the *Hauck* plaintiffs as to AMD. *See* Ex. 1, ¶ 186 (AMD “concealed from and failed to disclose [to the *Hauck* plaintiffs] . . . vital information concerning the Defect”); *see also id.* ¶ 66 (AMD failed to “disclose to consumers the fact that, as designed, their AMD CPUs were susceptible to microarchitectural attacks”).
- Plaintiffs allege that the “defects” affect almost every Intel processor sold for decades. *See* AC ¶ 7. So did the *Hauck* plaintiffs as to AMD. *See* Ex. 1, ¶ 162 (“[A]ll of the processors manufactured and sold by AMD since 1995 contain design flaws[.]”).
- Plaintiffs allege that exploits of these “defects” are untraceable. *See* AC ¶¶ 11, 636. So did the *Hauck* plaintiffs. *See* Ex. 1, ¶ 3 (“[N]either the CPU nor the consumer are aware that the CPU’s microarchitecture has been compromised.”).
- Plaintiffs allege that the “defects” stem from Intel sacrificing security for speed. *See* AC ¶¶ 9, 622. So did the *Hauck* plaintiffs as to AMD. *See* Ex. 1, ¶ 3 (“AMD sacrificed security for speed.”); *see also id.* ¶ 67 (consumers were “unaware that they were sacrificing the security of their sensitive information for increased processing speed”); *id.* ¶ 175 (AMD declined to address the defect “in order to achieve higher processing speeds”).
- Plaintiffs allege that the “defects” are inconsistent with Intel’s marketing statements about security. *See* AC ¶¶ 499-502. So did the *Hauck* plaintiffs as to AMD. *See* Ex. 1, ¶¶ 92-94 (AMD “confirmed” it “employed ‘[s]tandards-based security features,’ which ‘help ensure sensitive data is protected 24/7/365.’” “AMD claimed it ‘has you covered,’” and that “AMD’s robust silicon-level security features are competitive, consistent, and comprehensive.” (emphasis in original) (internal quotation marks omitted)).
- Plaintiffs allege that Intel was aware of research detailing potential side-channel vulnerabilities in its designs. *See* AC ¶¶ 516-27. So did the *Hauck* plaintiffs as to AMD. *See* Ex. 1, ¶¶ 125-54 (discussing many of the same papers cited here).
- Plaintiffs allege that this research was too technical for consumers to follow. *See* AC ¶ 528. So did the *Hauck* plaintiffs. *See* Ex. 1, ¶ 158 (“[O]rdinary consumers would not have been aware of, have access to, or even have sufficient expertise to understand the ramification of much of the university and industry research.”).
- Plaintiffs allege that the vulnerability mitigations were buggy and caused problems. *See* AC ¶ 657. So did the *Hauck* plaintiffs. *See* Ex. 1, ¶ 173 (patches “created

problems beyond a performance penalty, such as putting computers into a continuous reboot cycle,” or even “rendering them inoperable”).

- Plaintiffs allege that the mitigations do not fix the “defects.” *See* AC ¶¶ 22, 652-53. So did the *Hauck* plaintiffs. *See* Ex. 1, ¶ 166 (“[T]here is no way to completely eliminate the security vulnerabilities [the Defect] creates without redesigning the processor.”); *id.* ¶ 174 (“[T]he only long-term fix for the Defect is to totally redesign the CPUs[.]”).
- Plaintiffs allege that the mitigations result in performance penalties. *See* AC ¶¶ 655, 659. So did the *Hauck* plaintiffs—indeed, they alleged as much as a 30-50% slowdown caused by the mitigations. *See* Ex. 1, ¶ 170 (citing “a ballpark figure of *five to 30 per cent slow down*” (emphasis in original)); *id.* ¶ 171 (“[T]he performance penalty from mitigation can be *up to 50% . . .*”). The *Hauck* plaintiffs contended that the security vulnerabilities and the performance impact of mitigations rendered AMD’s processors unmerchantable. *Id.* ¶ 326.

The Ninth Circuit found no fraud or unfairness in these allegations and affirmed the dismissal with prejudice of the claims in *Hauck*, which are substantively identical to the claims here.

### STANDARD OF REVIEW

To survive a motion to dismiss under Rule 12(b)(6), a complaint must contain sufficient factual matter, accepted as true, to “state a claim to relief that is plausible on its face.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). While the Court must accept well-pleaded allegations as true and draw reasonable inferences in favor of the plaintiff, it should not credit legal conclusions couched as factual allegations. *Ashcroft v. Iqbal*, 556 U.S. 662, 678-79 (2009). Nor should it “accept allegations that are merely conclusory, unwarranted deductions of fact, or unreasonable inferences.” *Ward v. Bolek*, 2013 WL 145828, at \*1 (D. Or. Jan. 14, 2013); *see also Moss v. U.S. Secret Serv.*, 572 F.3d 962, 971-72 (9th Cir. 2009).

In addition to the allegations of the complaint and facts subject to judicial notice, in deciding a motion to dismiss, the Court may consider, “in [their] entirety,” documents incorporated into the complaint by reference (such as the academic articles Plaintiffs quote and

cite). *In re NVIDIA Corp. Sec. Litig.*, 768 F.3d 1046, 1052, 1058 n.10 (9th Cir. 2014) (internal quotation marks omitted). This rule “prevents plaintiffs from selecting only portions of documents that support their claims, while omitting portions of those very documents that weaken—or doom—their claims.” *Khoja v. Orexigen Therapeutics, Inc.*, 899 F.3d 988, 1002 (9th Cir. 2018).

As the deficiencies in Plaintiffs’ theory cannot be cured by amendment, dismissal with prejudice is appropriate. *See, e.g., Zucco Partners, LLC v. Digimarc Corp.*, 552 F.3d 981, 1007 (9th Cir. 2009).

## ARGUMENT

### **I. PLAINTIFFS FAIL TO STATE A FRAUD CLAIM UNDER CALIFORNIA LAW (COUNTS I-IV).**

This Court previously found that even if Plaintiffs had standing, Plaintiffs’ prior complaint would have failed to state a claim for their California fraud-based causes of action.<sup>13</sup> Op. & Order Granting Mot. to Dismiss 34-35 (“MTD Order”), ECF No. 178. Plaintiffs have added nothing to change that conclusion. *E.g.*, AC ¶¶ 41, 47; *supra* pp. 9-10. In light of its prior reasoning and *Hauck*, the Court should dismiss Plaintiffs’ fraud-based claims under the common law (Count I), CLRA (Count II), UCL (Count III), and FAL (Count IV).<sup>14</sup>

---

<sup>13</sup> Intel reserves the right to argue that California law cannot govern claims by non-California persons. *See Mazza v. Am. Honda Motor Co.*, 666 F.3d 581, 594 (9th Cir. 2012).

<sup>14</sup> The CLRA prohibits “unfair methods of competition and unfair or deceptive acts or practices.” Cal. Civ. Code § 1770(a). The UCL prohibits any “unlawful, unfair or fraudulent business act or practice.” *Rojas-Lozano v. Google, Inc.*, 159 F. Supp. 3d 1101, 1117 (N.D. Cal. 2016) (internal quotation marks omitted). And the FAL prohibits any statement “which is untrue or misleading, and which is known, or which by the exercise of reasonable care should be known, to be untrue or misleading.” *Elias v. Hewlett-Packard Co.*, 903 F. Supp. 2d 843, 853 (N.D. Cal. 2012) (quoting Cal. Bus. & Prof. Code § 17500). “The standard for all three statutes is the ‘reasonable consumer’ test[.]” *Id.* at 854 (citation omitted). Because they rely on the same standards,

**A. Plaintiffs Allege No Actionable Omissions.**

**1. Plaintiffs Fail To Satisfy Rule 9(b) as to the Nature of Any Defect.**

Both common law and statutory claims sounding in fraud must satisfy Rule 9(b)'s particularity requirement. *Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1103-04 (9th Cir. 2003). *Hauck* explained what Rule 9(b) requires when the alleged fraud is a failure to disclose a design choice that turns out, years later, to be exploitable through novel security vulnerabilities. In that case, Rule 9(b) requires the plaintiff to “allege the nature of the defect” with particularity. 2020 WL 2510754, at \*2. To plead the “nature of the defect,” a plaintiff must identify a specific vulnerability, e.g., “Spectre-like attacks in particular,” and may not rely on allegations that processor caches “are vulnerable to side-channel attacks generally” or are vulnerable generally “because of [] some other subset of their features.” *See id.* Thus, the Ninth Circuit completely rejected the plaintiffs’ fundamental strategy of defining a “subset of . . . features” as a “defect” with the benefit of hindsight. *Id.*

Plaintiffs here have adopted the exact strategy the Ninth Circuit rejected in *Hauck*. Recognizing that Intel could not have been aware of Spectre, Meltdown, or any of the related vulnerabilities before their discovery starting in 2017, Plaintiffs instead define the alleged “defects” in Intel’s CPUs as two design features that later made the Spectre and Meltdown proofs of concept possible. *See* AC ¶¶ 4-6, 542, 613. But calling these features “defects” is just another way of restating Intel’s susceptibility to side-channel attacks generally or to as-yet-unknown attacks like Spectre or Meltdown. Before Intel had knowledge of a specific vulnerability like Spectre or Meltdown that could actually exploit its design, Intel cannot have

---

“courts often analyze these three statutes together.” *Id.* The same analysis also applies to common-law fraud by omission claims. *See Myers v. BMW of N. Am., LLC*, 2016 WL 5897740, at \*7 (N.D. Cal. Oct. 11, 2016).

been aware of any “defect” in that design. For instance, Plaintiffs allege that “Unauthorized Access” is a “defect” rooted in Intel’s design allowing speculative instructions to return real values because Intel CPUs “address unauthorized . . . memory requests [only when] the processor [is] ready to retire the instructions in program order.” AC ¶¶ 533, 621. Plaintiffs explain how the novel vulnerabilities capitalize on this design decision. AC ¶¶ 542-617. But they never explain how this design decision is dangerous *in the absence of a specific vulnerability to exploit it*. Indeed, their individual allegations expressly treat the term “Defects” as though it referred to the specific vulnerabilities discovered starting in 2017 rather than the underlying design choices. *See, e.g.*, AC ¶ 46 (“[H]ad Plaintiff known about the Defects in Intel’s CPUs *or that mitigations needed to address the Defects would materially impact the CPUs’ functionality and performance*, she would not have bought the laptop . . . or would have paid less for it.”).

That a researcher, working in controlled laboratory conditions, made the groundbreaking discovery of a brand-new class of security vulnerabilities in 2017, *more than a decade* after Plaintiffs allege Intel made the challenged design decisions, cannot mean that Intel defrauded, at the moment of purchase, *everyone* who purchased an Intel CPU from 2006 onward. AC ¶ 780. As the Ninth Circuit held, conduct is actionably deceptive only if it would cause a reasonable consumer to change her behavior, and, as a matter of law, no reasonable consumer would prefer that CPU manufacturers avoid performance-enhancing features in view of a “theoretical risk of a cybersecurity flaw.” *Hauck*, 2020 WL 2510754, at \*2. Nor, as a matter of law, would reasonable consumers plausibly believe their devices would be “completely impervious to novel cybersecurity threats.” *Id.* Under Plaintiffs’ theory, whenever a novel security vulnerability is discovered, the failure to have disclosed, years earlier, every design decision that ultimately



enabled that vulnerability, or all incremental academic research published along the way, would become fraudulent in retrospect. The limiting principle the Ninth Circuit recognized in *Hauck*, grounded in Rule 9(b), prevents such a result and requires the dismissal of all of Plaintiffs' omission-based claims for failure to identify a defect with particularity.

## **2. Plaintiffs Do Not Allege a Central Functional Defect.**

Even if Plaintiffs had satisfied Rule 9(b), their omission-based claims would still fail. *Hodsdon v. Mars, Inc.*, 891 F.3d 857 (9th Cir. 2018), requires a plaintiff claiming a fraudulent omission under California law to plead that (1) the omission is material; (2) the defect is central to the product's function; and (3) at least one of the *LiMandri* factors is met. *Id.* at 863. The Court previously concluded that Plaintiffs had not alleged a central functional defect. MTD Order 34-35. Plaintiffs have not remedied that deficiency, which independently mandates the dismissal of Plaintiffs' California fraud-by-omission claims.

Plaintiffs do not and cannot allege that the design decisions at issue amount to a central functional defect in Intel's processors. To be a central functional defect, the allegedly defective product must be "incapable of use by any consumer." *Hodsdon*, 891 F.3d at 864. The Court previously noted that Plaintiffs failed to allege Intel's chips are incapable of use. MTD Order 34. The Amended Complaint does not change that analysis. Notwithstanding their new allegations of "freezing," "difficulty in multitasking," and the like, Plaintiffs' allegations still "show that they and others have been extensively using Intel's chips despite the alleged defect," which is fatal to their claim under *Hodsdon*. MTD Order 34; *see, e.g.*, AC ¶¶ 42-43, 48-49, 109-10.

Nor do Plaintiffs' allegations of performance degradation "plausibly show[] that an alleged decrease in performance was central to the functionality of any Named Plaintiff's CPU or rendered it incapable of use." MTD Order 35. Plaintiffs cannot overcome the obvious reality that Intel chips remain functional. Indeed, by alleging that the mitigations transform each of



their processors into the equivalent of a normally functioning earlier-generation processor, Plaintiffs expressly admit that their processors are *not* “incapable of use.” *Id.*; see AC ¶ 759.

Plaintiffs’ allegations are no different from the corresponding allegations in *Hauck*. Those plaintiffs alleged that the patches to their AMD processors caused significant slowdowns and “crashes” and that some plaintiffs no longer used their devices. Ex. 1 (*Hauck* Compl.) ¶¶ 10, 18, 27. Neither the district court nor the Ninth Circuit found those allegations sufficient to state a claim. 2020 WL 2510754, at \*3; *Hauck v. Advanced Micro Devices, Inc.*, 2019 WL 1493356, at \*17 (N.D. Cal. Apr. 4, 2019). In rejecting claims that AMD’s processors were unmerchantable (a standard that this Court observed is functionally identical to the *Hodsdon* test, see MTD Order 34), Judge Koh noted that, even assuming a 30% performance impact, the devices at issue were “certainly still operable,” though “a little less efficient.” *Hauck*, 2019 WL 1493356, at \*17. Thus, the plaintiffs “failed to allege that [their] processors lacked basic functionality as processors.” *Id.* The Ninth Circuit expressly affirmed that holding. 2020 WL 2510754, at \*3. The same conclusion applies here, for the same reasons, and supports dismissal of Plaintiffs’ omission claims under *Hodsdon*.

### **3. Plaintiffs’ Omission Claims Also Fail Because They Identify No Duty To Disclose Under the *LiMandri* Factors.**

To establish a duty to disclose—an indispensable element of an omission claim under California law—Plaintiffs must plead not only a central functional defect, but also one of the *LiMandri* factors. *Hodsdon*, 891 F.3d at 863. Those factors are: (1) the defendant was the plaintiff’s fiduciary; (2) the defendant had “exclusive knowledge” of the facts at issue; (3) the defendant “actively conceal[ed]” the facts at issue; or (4) the defendant made literally true but misleading statements (i.e., half-truths). *LiMandri v. Judkins*, 60 Cal. Rptr. 2d 539, 543 (Ct. App. 1997) (internal quotation marks omitted). Plaintiffs do not allege that Intel had a fiduciary

relationship with any Plaintiff. Nor are the other three factors satisfied, for the same reasons as in *Hauck*.

*i. Exclusive Knowledge*—*Hauck* held that the plaintiffs in that case did not satisfy this *LiMandri* requirement because, although they alleged that “AMD was aware of some of the vulnerabilities created by its design choices,” they did not “plausibly allege that AMD knew of the specific vulnerability identified in their second amended complaint until that vulnerability was disclosed to AMD in June 2017.” 2020 WL 2510754, at \*2. Thus, just as allegations of an undisclosed vulnerability to “side channel attacks generally” are not sufficient to plead fraud, only knowledge of a *specific vulnerability like Spectre or Meltdown* can support a duty to disclose. *See id.*

For the same reasons, Plaintiffs here fail to allege that Intel had knowledge, exclusive or otherwise, of any “defect” in its design. They allege the uncontroversial proposition that Intel knew more about its chip design than consumers did, and that Intel knew about academic papers discussing the theoretical possibility of side-channel vulnerabilities related to speculative execution and cache memory. *E.g.*, AC ¶ 516. But they do not and cannot allege that Intel knew that its design choices could be leveraged through a new class of vulnerabilities that were discovered more than a decade later by Google Project Zero.

And *Hauck* is no outlier in this regard. Indeed, the cases clarify that California’s fraud-based statutes require a defendant’s knowledge not only of its product’s design (something every manufacturer knows by definition), but also of how that design is actually defective. For example, in *Wilson v. Hewlett-Packard Co.*, the Ninth Circuit rejected the plaintiffs’ attempt to plead Hewlett-Packard’s knowledge of a defect in its design by pleading that Hewlett-Packard’s “inadequate Design for Reliability put HP on notice that [its] Laptops were and are seriously

defective.” 668 F.3d 1136, 1147 (9th Cir. 2012) (internal quotation marks omitted). That was not enough, because those plaintiffs failed to plead that HP knew *about a supposed defect*. The Ninth Circuit noted that mere allegations that “defendants were in a superior position to know the truth” about their own products, or that defendants had “exclusive knowledge as the manufacturer” were insufficient. *Id.* (internal quotation marks and citations omitted).

Plaintiffs cannot obfuscate this pleading defect by pejoratively renaming elements of Intel’s design. “Unauthorized Access” and “Incomplete Undo” are not security vulnerabilities. Plaintiffs themselves allege that they are performance-enhancing design features exploitable via *later-discovered* vulnerabilities like Spectre and Meltdown. The Complaint cites academic papers describing *potential* side-channel risks associated with those features, but Plaintiffs do not allege that any of these earlier papers identified Spectre, Meltdown, or any other member of the groundbreaking class of specific vulnerabilities first discovered in 2017. *Hauck* correctly rejected precisely this approach: Plaintiffs cannot allege a “defect” merely by pointing to “some . . . subset of [processor] features” or to Intel CPUs’ vulnerability “to side-channel attacks generally” rather than “Spectre-like attacks in particular.” 2020 WL 2510754, at \*2.

Equally irrelevant is the allegation that Intel made design choices different from other processor manufacturers. It simply makes no difference that one of the two design features Plaintiffs call “defects” is allegedly unique to Intel. AC ¶ 621. Both “Unauthorized Access” and “Incomplete Undo” were design decisions allegedly made to improve performance; both were present in Intel CPUs for more than a decade before researchers discovered the specific vulnerabilities at issue here; and both are said to allow an attacker to leverage speculative execution in a manner that may reveal confidential information. *See* AC ¶¶ 9, 440, 467, 473. *Hauck* involved the same fundamental scenario as to one of those exact design features—

researchers discovering a previously unknown way to manipulate processor design features to demonstrate a vulnerability. Under those facts, the plaintiffs could not plead AMD’s “exclusive knowledge of a defect” under *LiMandri*, and that reasoning applies here.

**ii. Active Concealment**—The Ninth Circuit ruled in *Hauck* that those plaintiffs failed to satisfy the *LiMandri* “active concealment” prong for the same reasons that they failed to meet the “exclusive knowledge” prong: they failed to “plausibly allege that AMD ‘suppresse[d]’ material facts regarding th[e] specific defect.” 2020 WL 2510754, at \*2 (citation omitted) (first alteration in original). That conclusion applies equally here. Because Intel did not know of any “specific” vulnerability, it could not have “concealed” anything, let alone done so “actively.”

**iii. Half-Truths**—Plaintiffs fail to allege any “half-truths” that could satisfy the final *LiMandri* factor, as *Hauck* confirms. Although Plaintiffs allege that Intel’s statements concerning security were false or misleading, no Named Plaintiff claims to have seen *any* Intel representation *concerning security*. See AC ¶¶ 499-501. Rather, each pleads that they “heard and/or read that Intel processors were the world’s fastest” or near-identical statements, and that “[i]mplicit” in those representations about performance was that the processor “would deliver such performance securely.” E.g., AC ¶ 41. But in *Hauck*, the Ninth Circuit concluded as a matter of law that none of AMD’s statements about performance was “likely to mislead consumers acting reasonably in the circumstances to their detriment, given that such consumers would not plausibly believe that AMD’s [performance] representations were premised on any implicit security assurances.” 2020 WL 2510754, at \*2 (dismissing analogous claims under Florida and Massachusetts law). The same analysis and dispositive conclusion apply here. Statements about performance do not carry “implicit security assurances,” so Plaintiffs’ theory of implicit misrepresentations about security is invalid as a matter of law.

Even if any Named Plaintiff had actually seen an Intel representation about security, no representation identified in the Amended Complaint is actionable, under this Court’s and *Hauck*’s reasoning. Plaintiffs repeatedly assert that Intel led reasonable consumers to expect “that the computing device being purchased would be secure and *free* from potential exploits.” *E.g.*, AC ¶ 29. But as the Court already observed, consumers cannot expect to be free from “any and all” security vulnerabilities. MTD Order 13, 17-18 (finding “Plaintiffs have not sufficiently alleged their reasonable expectations for data security”). *Hauck* reached the same conclusion, holding that AMD’s statements about security could not have led reasonable consumers to believe that “their devices would be completely impervious to novel cybersecurity threats.” 2020 WL 2510754, at \*2. Intel’s security statements are indistinguishable from AMD’s and cannot serve as a basis for an actionable fraud claim. *Compare* AC ¶¶ 499-501 (Intel chips were “secure to the core” and allowed consumers to feel “safe and secure at home”), *with* Ex. 1 (*Hauck* Compl.) ¶¶ 62, 94, 99 (AMD “help[ed] ensure sensitive data is protected 24/7/365” and “has you covered” with “robust silicon-level security features [that] are competitive, consistent, and comprehensive”).

**4. Plaintiffs Fail To Plead that Intel’s Alleged Omissions Were Material to Reasonable Consumers.**

*Hauck* provides a further independent ground to dismiss Plaintiffs’ omission-based claims—the alleged omissions were not material, as California law requires. *See Hodsdon*, 891 F.3d at 863. “Materiality exists if the omitted information would cause a reasonable consumer to behave differently if he or she were aware of the information.” *E.g.*, *Hovsepian v. Apple Inc.*, 2009 WL 5069144, at \*3 (N.D. Cal. Dec. 17, 2009); *accord Hauck*, 2020 WL 2510754, at \*2 (applying same standard under Florida and Massachusetts law). Plaintiffs fail to plausibly allege

that Intel’s alleged omissions would have deceived a reasonable consumer—i.e., that those alleged omissions were materially misleading—for three independent reasons.

*First*, to plead that the omitted information would cause a reasonable consumer to behave differently, Plaintiffs must plausibly allege that the omitted information was inconsistent with a reasonable consumer’s expectations. *See, e.g., Punian v. Gillette Co.*, 2016 WL 1029607, at \*15 (N.D. Cal. Mar. 15, 2016). As the Court previously held in the context of standing, Plaintiffs’ prior Complaint never identified “the parties’ bargain that Intel did not meet” and never alleged “that they would have sacrificed . . . processing speed for additional security against theoretical vulnerabilities.” MTD Order 17-18; *cf. id.* at 33 (noting that the Court would require “more allegations from Plaintiffs about their expectations and alleged bargain relating to the security vulnerabilities”). The Amended Complaint does not remedy that deficiency. Plaintiffs do not provide the Court with any plausible explanation of the supposed security bargain they expected. Instead, they uniformly assert that, at purchase, they expected their devices to be “*free* from potential exploits.” *E.g.*, AC ¶ 47. Thus, rather than address the Court’s concern, Plaintiffs continue to insist that they expected both perfect security *and* undiminished performance, indefinitely. *Id.* *Hauck* confirms that no *reasonable* consumer could have expected such a bargain. 2020 WL 2510754, at \*2.<sup>15</sup>

*Second*, based on *Hauck*’s reasoning, Plaintiffs have not and *cannot* plausibly identify any omitted information that would have changed a reasonable consumer’s behavior had it been

---

<sup>15</sup> Plaintiffs’ failure to specify the nature of their expected bargain is another, independent basis to conclude that their omission-based claims do not satisfy the particularity requirement of Rule 9(b). *See, e.g., Hovsepian*, 2009 WL 2591445, at \*3 (“[G]eneralized allegations with respect to consumer expectations are insufficient to meet Rule 9(b)’s heightened pleading requirements.”). The Amended Complaint never states, for example, what degree of security Plaintiffs *reasonably* expected, or what amount of performance they would have traded for that degree of security.

disclosed at the time of purchase. *Hauck* held that those plaintiffs could not plausibly allege they would have sacrificed the performance benefits of AMD’s processor design because of the “theoretical risk of a cybersecurity flaw that has not yet been successfully exploited.” 2020 WL 2510754, at \*2. The same is true here, because Plaintiffs allege nothing more than “theoretical risk[s]” prior to the discovery of Spectre and Meltdown. *See supra* pp. 6-8, 14-16, 17-21.

*Finally*, although the Amended Complaint conspicuously omits the five prior Named Plaintiffs who purchased after public disclosure of Spectre and Meltdown, those five consumers—and millions of other purchasers since the widespread public disclosure of Spectre and Meltdown in January 2018—remain members of the putative class. AC ¶ 780; *see* MTD Order 12. By alleging that these purchasers *after* that widespread disclosure *also* overpaid for Intel processors, Plaintiffs fatally undermine their own materiality allegations. *Cf. Noll v. eBay Inc.*, 2013 WL 2384250, at \*4 (N.D. Cal. May 30, 2013) (discounting allegations of reliance on an omission when plaintiffs did not change behavior after learning allegedly omitted facts). *Hauck*’s dismissal of the Massachusetts Consumer Protection Act omission claim by a plaintiff who bought after public disclosure of the novel vulnerabilities in January 2018 underscores this point; his purchase *after* the vulnerabilities became public knowledge demonstrated that AMD’s alleged nondisclosure *could not have* affected his behavior. *See* 2020 WL 2510754, at \*3. So too here: Plaintiffs’ allegations that millions of class members, with full knowledge of Spectre, Meltdown, and their variants, continue to buy Intel-based devices at their market price undercuts any allegation that those specific vulnerabilities, let alone the “Unauthorized Access” and “Incomplete Undo” design features standing alone, are material to reasonable consumers.<sup>16</sup>

---

<sup>16</sup> Because Plaintiffs have failed to plausibly allege materiality, they also have failed to allege reliance, which is an element of each of Plaintiffs’ omission-based claims under California law. *See Noll v. eBay Inc.*, 2013 WL 2384250, at \*4 (N.D. Cal. May 30, 2013). To allege reliance,

**B. Plaintiffs Fail To State a Claim Based on Affirmative Misrepresentations.**

No Named Plaintiff alleges seeing a single Intel statement regarding the security of its processors, or anything specific about processor performance. Thus, Plaintiffs fail to satisfy Rule 9(b), and the Court can dispose of any affirmative misrepresentation claim on that ground alone. For the same reason, Plaintiffs cannot satisfy the reliance element of an actionable misrepresentation claim. *Sud v. Costco Wholesale Corp.*, 229 F. Supp. 3d 1075, 1084 (N.D. Cal. 2017), *aff'd*, 731 F. App'x 719 (9th Cir. 2018). But even setting those issues aside, *Hauck's* reasoning forecloses any claim under California common law, the CLRA, the UCL, or the FAL that Intel made affirmative misrepresentations regarding either security or performance.

**1. No Plaintiff Alleges Viewing Any Specific Misrepresentation.**

The Named Plaintiffs formulaically recite that when buying their devices, they “reviewed and relied on the information about the laptop and Intel processor that was displayed” online or in the store. *See, e.g.*, AC ¶¶ 41, 47. Plaintiffs fail to allege even one fact about that “information”: what representations (if any) about either speed or security they supposedly saw; who provided this “information”; or how the unspecified “information” influenced their purchasing decision. The individual Named Plaintiffs separately allege in near-identical formulations that they “heard and/or read that Intel processors were the world’s fastest processors,” but do not identify any specific representation—much less one by Intel. *See id.* The entity Plaintiffs’ allegations, although employing different verbiage, are no more specific. *E.g.*, AC ¶ 73. Finally, Plaintiffs allege that they “[e]xpected the processor to function as Intel

---

Plaintiffs must plead, as relevant here, that awareness of the omitted information would have caused them to change their behavior. *Sud v. Costco Wholesale Corp.*, 229 F. Supp. 3d 1075, 1083 (N.D. Cal. 2017), *aff'd*, 731 F. App'x 719 (9th Cir. 2018). For the reasons just discussed, they cannot plausibly do so.



had advertised and represented.” But again, they do not even attempt to explain *what* Intel said that actually reached *them*. See, e.g., AC ¶¶ 41, 47. This failure to identify any specific representation viewed by any Named Plaintiff dooms the affirmative misrepresentation claims on at least two independent grounds.

First, Plaintiffs fail to satisfy the requirements of Rule 9(b). E.g., *Kearns v. Ford Motor Co.*, 567 F.3d 1120 (9th Cir. 2009). In *Kearns*, the Ninth Circuit upheld dismissal on Rule 9(b) grounds where a car purchaser alleged misrepresentations in Ford’s “televised national marketing campaign,” “sales materials found at the dealership,” and statements by “sales personnel,” but did not specify the content of any advertisement or sales material *that he viewed* and “which sales material *he relied upon* in making his decision.” *Id.* at 1125-26. The plaintiff alleged he was “told” that the certified vehicles “were the best used vehicles available,” but the Ninth Circuit found it fatal that the plaintiff did not “specify *who* made this statement or *when* this statement was made.” See *id.* at 1126 (internal quotation marks omitted). Thus, the plaintiff “failed to articulate the who, what, when, where, and how of the misconduct alleged.” *Id.*

Plaintiffs’ claims here fail for the same reason. Named Plaintiffs have not alleged the content of any online or in-store “information” that *they* viewed and that *they* allegedly relied on in making purchasing decisions.<sup>17</sup> Plaintiffs allege that they “heard and/or read that Intel processors were the world’s fastest,” that they had “superior performance, speed, and security,” or near-identical phrases. E.g., AC ¶¶ 41, 47, 78. But like the plaintiff in *Kearns*, they do not

---

<sup>17</sup> See, e.g., *Tabler v. Panera LLC*, 2020 WL 3544988, at \*8 (N.D. Cal. June 30, 2020) (dismissing under Rule 9(b) where plaintiff “merely identifies a range of representative advertisements that Plaintiff alleges to be misleading, but Plaintiff provides no indication of which statements, if any, Plaintiff herself relied upon”); *Garcia v. Sony Comput. Entm’t Am., LLC*, 859 F. Supp. 2d 1056, 1063 (N.D. Cal. 2012) (plaintiff failed to satisfy Rule 9(b) where he did “not specifically aver” he “relied on th[e] particular statements” on product packaging and website “or even expressly state that he was aware of them”).

specify “who made [these] statement[s] or when [these] statement[s] [were] made.” 567 F.3d at 1126. The affirmative misrepresentation claims should be dismissed for failure to satisfy Rule 9(b). *Id.*

*Second*, for these same reasons, Plaintiffs have failed to plead reliance on any misstatement, which California law requires for an affirmative misrepresentation claim. *See, e.g., Great Pac. Sec. v. Barclays Cap., Inc.*, 743 F. App’x 780, 783 (9th Cir. 2018) (“Plaintiffs alleging claims under the FAL and UCL are required to plead and prove actual reliance on the misrepresentations or omissions at issue.”); *Kearns*, 567 F.3d at 1126; *Garcia v. Sony Comput. Entm’t Am., LLC*, 859 F. Supp. 2d 1056, 1067 & n.6 (N.D. Cal. 2012) (same for CLRA claim). Because Plaintiffs fail to allege any specific representations they relied on in making their purchases, they can state no affirmative misrepresentation claims.

## **2. *Hauck’s Reasoning Forecloses Plaintiffs’ Affirmative Misrepresentation Claim as a Matter of Law.***

Even if some Named Plaintiff had alleged seeing Intel’s security-related statements identified in the Amended Complaint, none of those security statements supports a claim for affirmative misrepresentation in light of *Hauck*. The *Hauck* plaintiffs pointed to AMD’s claims to have “[s]trong, hardware-based security,” its assertion that its devices “help ensure sensitive data is protected 24/7/365,” and its statement that “AMD’s robust silicon-level security features are competitive, consistent, and comprehensive,” among numerous others. Ex. 1 (*Hauck* Compl.) ¶¶ 92, 94. The Ninth Circuit held as a matter of law that none of those statements was “likely to mislead consumers acting reasonably in the circumstances” because “consumers would not plausibly believe . . . that their devices would be completely impervious to novel cybersecurity threats.” 2020 WL 2510754, at \*2 (internal quotation marks omitted) (applying Florida and Massachusetts law). California applies the same reasonable-consumer test to

affirmative misrepresentations. *See id.*; *see also Ebner v. Fresh, Inc.*, 838 F.3d 958, 965 (9th Cir. 2016) (affirmative misrepresentation “claims under the California consumer protection statutes are governed by the ‘reasonable consumer’ test,” which requires showing “more than a mere possibility,” but a “probability,” that “a significant portion of the general consuming public” is “likely to be deceived”). The statements by Intel that Plaintiffs identify, and that the Court previously discussed, *see* MTD Order 53, are indistinguishable from the AMD statements that the *Hauck* court correctly held were not materially false or misleading as a matter of law.<sup>18</sup>

The same analysis applies to any allegation that Intel’s performance claims misled Plaintiffs. None of the Named Plaintiffs allege that their devices failed to provide any promised level of performance at the time of purchase. Recognizing this, the Named Plaintiffs allege instead that “[i]mplicit” in Intel’s (unidentified) representations “was that its processor would deliver such performance securely.” *See, e.g.*, AC ¶¶ 41, 47; *see also id.* (“Any reasonable consumer would expect that the computing device being purchased would be secure and free from potential exploits.”). Those allegations fly in the face of *Hauck*, which properly rejected the premise that *performance* representations contain implicit *security* promises as well as the idea that reasonable consumers expect perfect security. 2020 WL 2510754, at \*2.

In any event, developments *after* the purchase of a device cannot retroactively falsify statements that were true at the time of sale. In *Yastrab v. Apple, Inc.*, 173 F. Supp. 3d 972 (N.D. Cal. 2016), the court dismissed a complaint alleging that a software update disabled iPhones’ WiFi capability, where the plaintiffs had identified no statements at the time of purchase

---

<sup>18</sup> Another district court, in dismissing a putative securities class action against Intel arising from the discovery of Spectre and Meltdown, held that materially identical statements about security were nonactionable under the securities laws. *In re Intel Corp. Sec. Litig.*, 2019 WL 1427660, at \*9 (N.D. Cal. Mar. 29, 2019).

promising that updates would never affect device capabilities. *Id.* at 979, 981. And in *Garcia v. Sony Computer Entertainment America, LLC*, the court dismissed a complaint alleging that newer games were incompatible with, and thus damaged, PlayStation 3 hardware. 859 F. Supp. 2d at 1063. The court held that Sony’s time-of-sale representations about software compatibility were not misleading because Sony lacked “clairvoyance as to unspecified, future technological advancements in the field.” *Id.* Here, Plaintiffs claim to have expected that each of their devices “would retain all of its operating characteristics throughout its useful life.” *E.g.*, AC ¶¶ 46, 52. But reasonable consumers understand that their devices will receive regular updates that put increasing demands on hardware, impacting performance over time. *See In re Apple Inc. Device Performance Litig.*, 347 F. Supp. 3d 434, 461 (N.D. Cal. 2018) (reasonable consumers understand that newer software will demand more power and strain battery); *see also Garcia*, 859 F. Supp. 2d at 1065 (reasonable consumers understand that over time, hardware may have increasing difficulty coping with demands placed on it). Thus, even if any Named Plaintiff had identified a specific performance claim she relied on in making a purchase, no Named Plaintiff could plausibly allege that any such statement was false or misleading.

**C. Plaintiffs Cannot Pursue Equitable Remedies Under the California Statutes.**

Plaintiffs’ UCL and FAL claims (Counts III and IV), and their claim for equitable relief under the CLRA (Count II), fail for a further reason. As the Ninth Circuit recently held, Plaintiffs cannot pursue UCL and FAL claims without pleading that they lack an adequate remedy at law. *Sonner v. Premier Nutrition Corp.*, 962 F.3d 1072, 1076, 1081 (9th Cir. 2020) (affirming dismissal with prejudice under Rule 12(b)(6)). Here, Plaintiffs have not, *and cannot*, do so. Indeed, Plaintiffs plead quite the opposite: they allege precisely the same course of conduct and operative facts to support both their claims for damages and their claims for equitable remedies. *Compare*,

*e.g.*, AC ¶ 803 (allegations as to common-law fraud), *with, e.g.*, AC ¶ 828 (allegations as to UCL). Their claims for equitable relief, including for restitution, should be dismissed.

In *Sonner*, the trial court granted a motion to dismiss equitable restitution claims under the UCL and CLRA where, as the Ninth Circuit noted, “the operative complaint d[id] not allege that [the plaintiff] lacks an adequate legal remedy” and the claimed basis for equitable restitution was the same as the theory for damages. 962 F.3d at 1081 (complaint that did not plead “the basic requisites of the issuance of equitable relief,” including “the inadequacy of remedies at law,” was properly dismissed (quoting *O’Shea v. Littleton*, 414 U.S. 488, 502 (1974))). In affirming that dismissal, the Ninth Circuit held that federal courts sitting in diversity are required to apply “traditional equitable principles,” including “the requisite inadequacy of legal remedies . . . when a party requests restitution under the UCL and CLRA.” *Id.* at 1078, 1081 (citing *Guar. Tr. Co. v. York*, 326 U.S. 99 (1945)). As the Ninth Circuit recognized, “California courts have held that ‘the UCL provides only for equitable remedies.’” *Id.* at 1076 n.2 (citation omitted). And the California Supreme Court has held the same for the FAL. *Nationwide Biweekly Admin., Inc. v. Superior Court*, 462 P.3d 461, 485 (Cal. 2020) (“[A] civil action under the UCL and FAL is equitable rather than legal in nature.”). Plaintiffs accordingly seek only equitable relief under the UCL and FAL and also seek equitable remedies under the CLRA. *See* AC ¶¶ 834, 845; *see also* AC ¶ 822. Because the Amended Complaint nowhere pleads that Plaintiffs lack a remedy at law—nor could it—the Court should dismiss those claims.<sup>19</sup>

---

<sup>19</sup> *Sonner* also dooms Plaintiffs’ unjust enrichment/quasi-contract claim. *See infra* note 22.

## II. PLAINTIFFS FAIL TO STATE A CLAIM FOR UNFAIR OR UNLAWFUL TRADE PRACTICES UNDER CALIFORNIA LAW (COUNT III).

### A. Plaintiffs Do Not Plead Any Unfair Trade Practice.

Plaintiffs allege two purportedly unfair business practices. *First*, they assert that Intel’s CPU design choices unfairly “sacrific[ed] security for speed for the purpose of increasing profits.” AC ¶ 828(a)-(d). But *Hauck* rejected that same argument, and California law prohibits a no-injury strict liability claim dressed up as a consumer-protection UCL claim. *Second*, they contend that Intel made misrepresentations and material omissions regarding the security and performance of its CPUs—in other words, the same theory underlying their fraud claims. AC ¶ 828(e)-(g). But Plaintiffs may not save their deficient fraud claims by repackaging them as claims for unfair trade practices.

As the Court previously recognized, the balancing test that governs Plaintiffs’ “unfair” prong claim “asks whether the alleged practice is immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers and requires the court to weigh the utility of the defendant’s conduct against the gravity of the harm to the alleged victim.” MTD Order 45-46. While the unfairness of a business practice may be a question of fact *if supported by appropriate allegations*, federal courts do not hesitate to dismiss such claims under Rule 12(b)(6) when “the complaint fails to allege facts showing that a business practice is unfair.” *Davis v. HSBC Bank*, 691 F.3d 1152, 1171 (9th Cir. 2012) (quoting *Bardin v. DaimlerChrysler Corp.*, 39 Cal. Rptr. 3d 634, 644 (Ct. App. 2006)) (internal quotation marks omitted); *see also, e.g., Apple Device*, 347 F. Supp. 3d at 464 (dismissing claim of unfair trade practices based on Apple software updates that allegedly hurt performance); *Elias v. Hewlett-Packard Co.*, 903 F. Supp. 2d 843, 858 (N.D. Cal. 2012) (dismissing claim of unfair trade practices in sale of laptops with allegedly defective design). The Court should dismiss Plaintiffs’ unfair practices claim here.

**1. *Hauck* Supports Dismissal of Plaintiffs’ Unfair-Practices Claim.**

In *Hauck*, the Ninth Circuit held that the plaintiffs failed to state a UCL claim for unfair trade practices against AMD. 2020 WL 2510754, at \*2. The Ninth Circuit first noted that it would address the “unfair” prong claim only “[t]o the extent” it was not “grounded in fraud.” *Id.* The court thus accepted Judge Koh’s holding that the *Hauck* plaintiffs’ “unfair” prong claim could not survive to the extent that it “overlap[ped] entirely” with their deficient “fraudulent” prong claim. *Hauck*, 2019 WL 1493356, at \*15 (internal quotation marks omitted); *see also*, *e.g.*, *Apple Device*, 347 F. Supp. 3d at 464. That holding follows from the Ninth Circuit’s prior conclusion that “failure to disclose information [the defendant] had no duty to disclose in the first place is not substantially injurious, immoral, or unethical.” *Hodsdon*, 891 F.3d at 867. The same is true here—Plaintiffs cannot advance a fraud-based “unfair” prong claim UCL claim where, as described above, they can allege no actionable misrepresentation or omission.

The Ninth Circuit then held that under the balancing test, too, the *Hauck* plaintiffs could not state an “unfair” prong claim based on AMD’s design choices. As the court explained, “[p]laintiffs have not plausibly alleged either the existence of false advertising or an actual violation of a privacy right, nor have they plausibly alleged that the harm represented by the theoretical risk of a cybersecurity flaw that has not yet been successfully exploited outweighs the other benefits of AMD’s processor design.” 2020 WL 2510754, at \*2.

There is no meaningful difference between the *Hauck* plaintiffs’ unfairness allegations and the allegations here. Plaintiffs here allege that Intel “sacrifice[ed] security for speed for the purpose of increasing profits, despite knowing about the attendant security vulnerabilities.” AC ¶ 828(b). *Hauck* rejected near-identical claims that AMD intentionally sacrificed security for performance to enhance its profits: “[The] Defect was the result of AMD’s decision to compromise the confidentiality of consumers’ most sensitive information to increase the speed

and performance levels of its CPUs. *In short, AMD sacrificed security for speed.*” Ex. 1 (*Hauck Compl.*) ¶ 3; *see also id.* ¶ 67 (“[C]onsumers purchased AMD CPUs throughout the Class Period unaware that they were sacrificing the security of their sensitive information for increased processing speed.”); *id.* ¶ 84 (AMD allegedly pursued performance at the expense of security “in order to gain market share”); *id.* ¶ 175 (“Defendant was aware of the defect in its processors but did not correct the defect prior to sale in order to achieve higher processing speeds in their products, which they then falsely marketed as defect-free.”).

Just as in *Hauck*, Plaintiffs cannot plausibly allege that the “theoretical risk of a cybersecurity flaw that has not yet been successfully exploited” outweighs the benefits of a processor design that, as they acknowledge, offered substantial performance benefits. *See, e.g.*, AC ¶ 533 (“Unauthorized Access” “enhance[d] the processor’s performance”); AC ¶ 507 (alleging Intel implemented both “Unauthorized Access” and “Incomplete Undo” “to achieve increased speed”); AC ¶¶ 682-88 (discussing importance of CPU performance to consumers).<sup>20</sup>

If Plaintiffs’ theory of unfairness is that Intel could have improved its design, but chose not to, that theory was presented and rejected in *Hauck* as well. *See* AC ¶ 828(d) (alleging Intel failed “to take steps to secure the CPU architecture from cache side-channel attacks”). The *Hauck* plaintiffs alleged that “despite AMD’s knowledge of how to design a secure system . . . AMD did nothing to address” the problems in its processors. Ex. 1 (*Hauck Compl.*) ¶ 67; *see also id.* ¶¶ 155-56 (alleging AMD knew about research proposals to improve microarchitecture security and took no action).

---

<sup>20</sup> Plaintiffs also have not successfully alleged “false advertising,” nor have they alleged any “actual violation of a privacy right” because none of them has suffered a data breach.



## 2. California Law Bars Plaintiffs’ “Unfair Design Choice” Theory.

Even independent of *Hauck*, Plaintiffs’ “unfair design choice” theory fails under established California law. In *Bardin v. DaimlerChrysler Corp.*, 39 Cal. Rptr. 3d 634 (Ct. App. 2006), the plaintiffs alleged that Chrysler deliberately designed its cars with cheaper parts to increase profits and gain market share. *Id.* at 637. The parts allegedly fell below the industry standard, and the plaintiffs claimed they were not aware of Chrysler’s design tradeoff at the time of purchase. *Id.* Nonetheless, the California Court of Appeal held, as a matter of law, that Chrysler’s design decision was not an unfair business practice in the absence of any physical injury, affirmative misrepresentation, or breach of warranty. *Id.* at 643-44.

Like *Hauck*, *Bardin* examined the substance rather than the label of the plaintiffs’ unfair business practices claim, and recognized that the plaintiffs were trying to pursue a strict products liability claim without alleging the physical injury or property damage such claims require. Strict liability doctrine ensures that consumers can be compensated for *physical* damages to themselves or their property without having to bargain for a warranty to that effect. But a consumer is not entitled to a guarantee “that [a] product will . . . match his economic expectations unless the manufacturer agrees that it will” by offering a warranty. *Seely v. White Motor Co.*, 403 P.2d 145, 151 (Cal. 1965). For this reason, *Bardin* held that a plaintiff may not use the UCL “unfair” prong as an end-run around the physical injury requirement of products-liability law. *See* 39 Cal. Rptr. 3d at 644.<sup>21</sup>

Plaintiffs’ unfair design choice theory, too, sounds in strict liability and therefore fails. A seller may be strictly liable for a design defect when “the foreseeable risks of harm posed by the

---

<sup>21</sup> The Court previously cited *Henryhand v. Dorel Juvenile Group*. 2017 WL 7806590 (C.D. Cal. Oct. 5, 2017). *Henryhand* involved allegations that the product at issue created a physical safety hazard and is thus consistent with the discussion here. *Id.* at \*7; *see* MTD Order 48.

product could have been reduced or avoided by the adoption of a reasonable alternative design by the seller.” *Trejo v. Johnson & Johnson*, 220 Cal. Rptr. 3d 127, 154 (Ct. App. 2017) (internal quotation marks omitted). This is exactly the argument Plaintiffs make in support of their unfair trade practices claim. *See, e.g.*, AC ¶ 828(c) (alleging that Intel committed an unfair trade practice by “[p]ermitting instruction execution in [] Intel CPUs without first performing and enforcing the appropriate memory access checks”). Under *Bardin*, this argument must be presented as a strict liability claim; it cannot advance as “unfairness.”

Plaintiffs posit that a product may be “defective,” and selling it may therefore be “unfair,” even if the product (i) is fit for ordinary use (i.e., does not breach any implied warranty), (ii) functions as the manufacturer represented at the time of sale (i.e., does not breach any express warranty), and (iii) poses no physical safety risk. They argue that Intel’s conduct was “unfair” even so, because, they claim, Intel traded (theoretical) security for (actual) speed. But design tradeoffs are inevitable in any manufactured product (such as the tradeoff between affordability and durability discussed in *Bardin*). And this is especially true for complex devices like computers and smartphones. *See, e.g., Apple Device*, 347 F. Supp. 3d at 461 (discussing tradeoff between smartphone performance and power consumption). On Plaintiffs’ view, however, every such decision could be an unfair business practice giving rise to benefit-of-the-bargain damages, if a buyer believes later that the tradeoff was “unfair.” A litigant could drag courts and juries into deciding the “right” level of security, performance, power consumption, durability, and so on for every manufactured product. That is not the law.

The notion that Intel “unfairly” prioritized CPU performance rings especially hollow in light of Plaintiffs’ repeated allegations that performance is of critical importance to computer consumers. *See, e.g.*, AC ¶ 683 (“Users *really* care about speed in interactive environments.”)

(emphasis in original); AC ¶ 687 (“When talking about responsiveness to performance requests, milliseconds matter.”). How can it be an unfair trade practice to prioritize a feature that Plaintiffs themselves allege is critical to consumers, especially where the alleged tradeoff is a design that gave rise to no specific known vulnerability for more than a decade? Plaintiffs have no answer.

Finally, the allegation that Intel acted “for the purpose of increasing profits” adds nothing because any design decision could be alleged to be profit-motivated. AC ¶ 828(b); *see, e.g., Bardin*, 39 Cal. Rptr. 3d at 643-44 (giving no weight to plaintiffs’ allegations that Chrysler’s allegedly unfair conduct was profit-motivated).

The Court should follow *Hauck* and *Bardin* and reject Plaintiffs’ attempt to shoehorn a no-injury products liability claim into the UCL.

**B. Plaintiffs Do Not Plead Any Unlawful Trade Practice.**

The UCL also prohibits “unlawful” business practices. Cal. Bus. & Prof. Code § 17200. Stating a claim under the “unlawful” prong requires an alleged violation of another “borrow[ed]” law. *See* MTD Order 44. Here, as in their prior Complaint, Plaintiffs rely on alleged violations of the CLRA and California common law, but they have stated no such claims. *Supra* pp. 13-30. The Court should dismiss the “unlawful” prong claims.

**III. PLAINTIFFS FAIL TO STATE A CLAIM FOR UNJUST ENRICHMENT OR QUASI-CONTRACT UNDER CALIFORNIA LAW (COUNT V).**

Plaintiffs’ final count under California law alleges a claim for “quasi contract or unjust enrichment.” AC ¶¶ 846-51. This claim relies on the same allegations as Plaintiffs’ other counts—that Intel “knowingly sacrificed security for speed” and failed to disclose that it had done so, depriving Plaintiffs of the benefit of their bargain. AC ¶¶ 848-50. But because all of

Plaintiffs' other claims fail, Plaintiffs cannot maintain an unjust enrichment or quasi-contract count.<sup>22</sup> The Court should dismiss Count V.

A claim for unjust enrichment or quasi-contract is valid only when “a defendant has been *unjustly* conferred a benefit.” *Astiana v. Hain Celestial Grp.*, 783 F.3d 753, 762 (9th Cir. 2015). Courts apply “traditional equitable principles” in determining whether *unjust* enrichment has occurred. *Yalley v. Liberty Life Assurance Co.*, 2019 WL 2710242, at \*7 (Cal. Ct. App. June 28, 2019) (quoting *Ghirardo v. Antonioli*, 924 P.2d 996, 1002 (Cal. 1996)). Thus, a plaintiff claiming unjust enrichment must ground her cause of action in traditional doctrines of equity. *See Hartford Cas. Ins. Co. v. J.R. Mktg., LLC*, 353 P.3d 319, 326 (Cal. 2015).

Recovery on this theory, then, ordinarily requires the plaintiff to plead an independently wrongful act. The cases cited in the Court's prior opinion are not to the contrary. *See Astiana*, 783 F.3d at 762 (cited at MTD Order 50) (false and misleading product labeling); *Prakashpalan v. Engstrom, Lipscomb & Lack*, 167 Cal. Rptr. 3d 832, 855 (Ct. App. 2014) (cited at MTD Order 51) (theft of settlement funds); *Himelsein Mandel Fund Mgmt., LLC v. Fortress Inv. Grp.*, 2019 WL 1395963, at \*15 (Cal. Ct. App. Mar. 28, 2019) (cited at MTD Order 50) (misappropriation of trade secrets and fraud).<sup>23</sup> The Court previously reasoned that Plaintiffs may be able to state

---

<sup>22</sup> Because Plaintiffs' unjust enrichment/quasi-contract claim seeks only equitable remedies, this claim should also be dismissed under the holding of *Sonner*, 962 F.3d at 1081. *See supra* pp. 28-30.

<sup>23</sup> In *Professional Tax Appeal v. Kennedy-Wilson Holdings, Inc.*, 239 Cal. Rptr. 3d 908 (Ct. App. 2018) (cited at MTD Order 50), the court allowed a quasi-contract claim to proceed based on traditional equitable principles as set forth in the Restatement of Restitution. *See id.* at 916. Here, Plaintiffs cannot invoke any such traditional principles of equity; nothing in the Restatement requires restitution of a product's purchase price in the absence of fraud, a deceptive, unfair, or unlawful trade practice, or a breach of warranty. And *Otworth v. Southern Pacific Transportation Co.*, 212 Cal. Rptr. 743 (Ct. App. 1985) (cited at MTD Order 51), *dismissed* an unjust enrichment claim for failure to allege “unjust” conduct.

an unjust enrichment or quasi-contract claim by stating a claim for unfair trade practices. *See* MTD Order 51. But as discussed above and consistent with *Hauck*, Plaintiffs cannot state such a claim, or any other valid cause of action against Intel. *Supra* pp. 13-35. Because Plaintiffs have established no wrongful act nor any foundation for their unjust enrichment or quasi-contract claim in traditional equitable principles, the Court should dismiss Count V.

#### **IV. PLAINTIFFS FAIL TO STATE A CLAIM FOR ANY BELLWETHER COUNT.**

For purposes of this motion, the Court ordered (per the parties' stipulation) that each side identify three statutory subclass claims to be briefed apart from the claims under California law. Pretrial Order No. 8, ECF No. 186. The parties picked Count XIV (Florida Deceptive and Unfair Trade Practices Act, "FDUTPA"), a count mislabeled as a second Count XIV (Illinois Consumer Fraud and Deceptive Business Practices Act, "ICFA"), Count XXXIV (New Jersey Consumer Fraud Act, "NJCFA"), Count XXXVI (New York General Business Law, "NYGBL"), Count XXXIX (Ohio Consumer Sales Practices Act, "OCSPA"), and Count XLVIII (Texas Deceptive Trade Practices Act, "TDTPA"). All these claims—whether for omissions, affirmative misrepresentations, "unfairness," or "unconscionability"—fail as a matter of law. Plaintiffs also cannot advance any claim for which there is no Named Plaintiff, as is the case for the OCSPA.

##### **A. Plaintiffs State No Bellwether Claim for Omissions.**

*First*, all bellwether omission claims should be dismissed for failure to satisfy Rule 9(b). As *Hauck* illustrates, no omission claim can satisfy Rule 9(b) based solely on the nondisclosure of a design choice independent of a specific vulnerability such as Spectre. *See supra* pp. 14-16. Rule 9(b) also requires Plaintiffs, under any state's law, to specify the details of the bargain Intel allegedly failed to fulfill. *See, e.g., Hovsepian*, 2009 WL 2591445, at \*3 ("[G]eneralized allegations with respect to consumer expectations are insufficient to meet Rule 9(b)'s heightened pleading requirements."). Plaintiffs have not done so.

*Second*, the reasoning of *Hauck* compels dismissal of omissions claims under the substantive provisions of each bellwether statute (independent of Rule 9(b)), because all require materiality. As *Hauck* explained, an FDUTPA claim requires an omission that is likely to mislead consumers “acting reasonably in the circumstances.” 2020 WL 2510754, at \*2 (quoting *PNR, Inc. v. Beacon Prop. Mgmt.*, 842 So. 2d 773, 777 (Fla. 2003)). *Hauck* expressly affirmed the dismissal of the plaintiffs’ FDUTPA omission claim because no reasonable consumer expects a device to be “completely impervious to novel cybersecurity threats,” and therefore the nondisclosure of a theoretical security vulnerability, as a matter of law, is not “likely to mislead” under the FDUTPA. *Id.* (internal quotation marks omitted). The same result follows in the other five states, too, all of which require that the information omitted be material.<sup>24</sup> As the alleged omission here—not disclosing information about theoretical security risks in performance-enhancing processor features—was not material as a matter of law, no omissions claim from any of the six bellwether states can advance.

*Third*, for an omissions claim all of the bellwether statutes require that the defendant *knew* the allegedly omitted facts at the time of sale.<sup>25</sup> The Named Plaintiffs from all bellwether

---

<sup>24</sup> See *Karpowicz v. Gen. Motors Corp.*, 1997 WL 413929, at \*6 (N.D. Ill. July 18, 1997) (omission is only actionable under the ICFA if it is *material*, meaning plaintiff would have acted differently had it been disclosed or the information was of the type on which a buyer would be expected to rely in purchasing); *Smajlaj v. Campbell Soup Co.*, 782 F. Supp. 2d 84, 99-100 (D.N.J. 2011) (NJCFRA requires plaintiff to plead that product failed to meet *objectively reasonable* expectations); *Gomez-Jimenez v. N.Y. Law Sch.*, 956 N.Y.S.2d 54, 58 (App. Div. 2012) (NYGBL omissions claim requires that defendant “alone possesse[d] *material* information that is relevant to the consumer and fail[ed] to provide this information” (citing, *e.g.*, *Oswego Laborers’ Local 214 Pension Fund v. Marine Midland Bank, N.A.*, 647 N.E.2d 741, 745 (N.Y. 1995))); *Grgat v. Giant Eagle, Inc.*, 135 N.E.3d 846, 850-51 (Ohio Ct. App. 2019) (OCSPA omissions claim requires allegations that *reasonable* consumer would have been deceived); Tex. Bus. & Com. Code § 17.46(b)(24) (TDTFA omissions claim requires non-disclosure of *material* information such that consumer would not have entered transaction had they known it).

<sup>25</sup> See *Hauck*, 2019 WL 1493356, at \*17 (under the FDUTPA “a manufacturer must have known of the defect at the time of sale for a plaintiff to state a claim for fraud by omission” (citing

states have not and cannot make such an allegation with respect to their purchases, because all Intel allegedly knew at that time was that its design features provided demonstrable performance benefits with—at most—theoretical security risks. *See supra* pp. 17-21.

*Fourth*, an omissions claim under the ICFA, NJCFA, and TDTPA require that the defendant intend that others rely on the concealment. *See* 815 Ill. Comp. Stat. 505/2 (requiring for an ICFA claim “intent that others rely upon the concealment, suppression or omission”); *Judge v. Blackfin Yacht Corp.*, 815 A.2d 537, 542 (N.J. Super. Ct. App. Div. 2003) (NJCFA omissions claim requires that the defendant “intentionally concealed the information [at issue] with the intention that [the] plaintiff would rely on the concealment”); Tex. Bus. & Com. Code § 17.46(b)(24) (TDTPA omissions claim requires allegation that defendant thereby “intended to induce” transaction). Intel could not have intended to mislead the Illinois, New Jersey, and Texas Named Plaintiffs by failing to disclose information where the only information it had at the time of those purchases—at most, knowledge of *theoretical* vulnerabilities—was immaterial as a matter of law. *Hauck*, 2020 WL 2510754, at \*2; *see Judge*, 815 A.2d at 543 (vacating judgment; “[t]here being no duty to disclose, there can be no finding” of the requisite intent).

---

*Matthews v. Am. Honda Motor Co.*, 2012 WL 2520675, at \*3 (S.D. Fla. June 6, 2012)); *Rockford Mem’l Hosp. v. Havrilesko*, 858 N.E.2d 56, 62 (Ill. App. Ct. 2006) (“[F]or a material omission to be actionable [under the ICFA], the plaintiff must establish that the fact concealed was *known* to the defendant at the time of the concealment.”); N.J. Stat. Ann. § 56:8-2 (NJCFA provision prohibiting “the *knowing*[] concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission”); *In re Sling Media Slingbox Advert. Litig.*, 202 F. Supp. 3d 352, 359-60 (S.D.N.Y. 2016) (granting motion to dismiss NYGBL omission claim when plaintiff failed to plead that defendant “had knowledge of the information [p]laintiffs allege it failed to disclose at the time [p]laintiffs made their purchases”); *Kondash v. Kia Motors Am., Inc.*, 2016 WL 11246421, at \*11 (S.D. Ohio June 24, 2016) (OCSPA omissions claim requires that plaintiff allege the “manufacturer knew of design defects and failed to disclose . . . defects [that] existed at the time of sale”); *Washburn v. Sterling McCall Ford*, 521 S.W.3d 871, 876 (Tex. App. 2017) (dealership could not be liable for omissions when it was unaware at time of sale of manufacturer’s warranty restriction; allegations that defendant “should have known” are insufficient).



*Fifth*, for an omissions claim to advance under the ICFA requires identifiable statements that could have contained the allegedly concealed information. *See De Bouse v. Bayer AG*, 922 N.E.2d 309, 315-16 (Ill. 2009) (plaintiff must point to a “direct statement[]” or “particular advertisement” containing “misleading statements *and material omissions*”). The Illinois Named Plaintiffs fail to identify any such statement. AC ¶¶ 108, 114.

*Finally*, an NYGBL omissions claim requires a “*manifested defect*.” *In re Gen. Motors LLC Ignition Switch Litig.*, 257 F. Supp. 3d 372, 429 (S.D.N.Y. 2017). Plaintiffs seek to define the alleged “defects” in Intel’s CPUs as the set of design features that a researcher (many years later, and three years *after* the New York Named Plaintiff purchased) discovered how to manipulate in a way that made the Spectre and Meltdown proofs of concept possible. However, the allegation that a superior design alternative existed, without more, does not establish a “manifested” defect. *See Frank v. DaimlerChrysler Corp.*, 741 N.Y.S.2d 9, 14, 16-17 (App. Div. 2002) (internal quotation marks omitted).<sup>26</sup> Under this standard, no “defect” has “manifested” here because the New York Named Plaintiff can claim no hack or breach of his now seven-year-old computer. As in *Hauck* and *Bardin*, *see supra* pp. 30-35, Plaintiff Apple cannot state an NYGBL claim solely because of his alleged dissatisfaction with Intel’s design choices.

---

<sup>26</sup> “Plaintiffs’ argument, basically, is that as an accident becomes foreseeably possible, upon the occurrence of certain contingencies, due to a design aspect of a product, the manufacturer must retrofit the product or otherwise make the consumer whole. However, under such a schematic, as soon as it can be demonstrated, or alleged, that a better design exists, a suit can be brought to force the manufacturer to upgrade the product or pay an amount to every purchaser equal to the alteration cost.” *Frank*, 741 N.Y.S.2d at 16-17.



**B. Plaintiffs State No Bellwether Claim for Affirmative Misrepresentations.**

*First*, like the omission claims, all of the state affirmative misrepresentation claims fail to satisfy Rule 9(b) and should be dismissed. As the Ninth Circuit interpreted Rule 9(b) in *Kearns*, any affirmative misrepresentation claim sounding in fraud must be supported by allegations of a specific allegedly misleading representation that the plaintiff heard or read. 567 F.3d at 1125-26; *supra* pp. 24-26. None of the Named Plaintiffs bringing the bellwether claims have identified any such misrepresentation. *See* AC ¶¶ 73, 80 (Florida), 108, 114 (Illinois), 193, 292, 298 (New Jersey), 205 (New York), 1296 (Ohio), 348 (Texas). All of these affirmative misrepresentation claims therefore should be dismissed for failure to meet federal pleading requirements.

*Second*, the same failure to identify a specific, allegedly misleading representation that the plaintiff reviewed compels the dismissal of all affirmative misrepresentation claims under the *substantive* provisions of each bellwether claim, for reasons independent of Rule 9(b). None of those statutes permits a plaintiff to advance a claim without identifying any misrepresentations that *she herself saw or heard*.<sup>27</sup>

---

<sup>27</sup> *See Hall v. Sea World Entm't, Inc.*, 2015 WL 9659911, at \*16 (S.D. Cal. Dec. 23, 2015) (FDUTPA plaintiff must “specifically allege that [she] viewed” or heard an allegedly deceptive advertisement prior to purchase); *De Bouse*, 922 N.E.2d at 316 (ICFA requires that “the plaintiff must actually be deceived by a statement or omission that is made by the defendant”; “[i]f a consumer has neither seen nor heard any such statement, then she cannot have relied on the statement and, consequently, cannot prove proximate cause”); *Rosenthal v. Sharkninja Operating LLC*, 2016 WL 7338535, at \*3, \*4 (D.N.J. Dec. 19, 2016) (NJCFRA requires “direct causal connection between the misrepresentation and the plaintiff’s defeated expectations,” such that a claim of exposure even to “pervasive” advertisements is not sufficient where a plaintiff alleges no “false fact, content of the alleged misleading material, [or] some specificity of what he saw” (internal quotation marks omitted)); *Szymczak v. Nissan N. Am. Inc.*, 2011 WL 7095432, at \*15 (S.D.N.Y. Dec. 16, 2011) (NYGBL claimant must “allege receipt of or exposure to the misleading practice”; dismissing claims for lack of specificity); *Woods v. Maytag Co.*, 2010 WL 4314313, at \*16 (E.D.N.Y. Nov. 2, 2010) (for an NYGBL claim, “general references to advertisements and statements will not be sufficient to allege a deceptive act or practice”); *Marlowe v. Nature’s Bounty Co.*, 2017 WL 2291683, at \*2 (N.D. Ohio May 25, 2017) (OCSPA requires plaintiff to allege that she “was aware of the alleged misrepresentation before or during the purchase” to satisfy the statute’s causation requirement); *Deburro v. Apple, Inc.*, 2013 WL

*Third*, an affirmative misrepresentation claim can proceed only where the alleged misrepresentation was material. As *Hauck* recognized in assessing the FDUTPA claim there, reasonable consumers would not believe that a performance representation is “premised on any implicit security assurances,” nor that their devices would be “impervious to novel cybersecurity threats.” 2020 WL 2510754, at \*2. Reasonable consumers understand that performance claims do not contain implicit security promises, and general security representations do not promise perfect security. *Supra* pp. 24-28. That dooms the FDUTPA claim, which requires statements that are “likely to mislead” consumers “acting reasonably in the circumstances.” *Id.* (quoting *PNR*, 842 So. 2d at 777). It also dooms the claims under every other bellwether statute, which similarly require materiality.<sup>28</sup>

---

5917665, at \*5 (W.D. Tex. Oct. 31, 2013) (TDTPA claim could not proceed where plaintiffs failed to allege “hav[ing] seen any of the representations listed in the [complaint] prior to purchasing [the product]”).

<sup>28</sup> See *Bober v. Glaxo Wellcome PLC*, 246 F.3d 934, 938 (7th Cir. 2001) (alleged misrepresentation must “create a likelihood of deception or . . . have the capacity to deceive” to be actionable under the ICFA); *Ibarrola v. Kind, LLC*, 83 F. Supp. 3d 751, 756 (N.D. Ill. 2015) (citing *Bober*, 246 F.3d at 940) (ICFA claims should be dismissed if challenged statements are “not misleading as a matter of law,” judged objectively from the standpoint of a reasonable consumer); *Popejoy v. Sharp Elecs. Corp.*, 2015 WL 5545067, at \*3 (D.N.J. Sept. 18, 2015) (NJCFA claim for affirmative misrepresentation requires allegations of misrepresentation “likely to deceive an average or reasonable customer” (equating New Jersey, California and other state statutory standards)); *Fink v. Time Warner Cable*, 714 F.3d 739, 741 (2d Cir. 2013) (per curiam) (NYGBL proscribes acts “likely to mislead a reasonable consumer acting reasonably under the circumstances”—an objective standard that may be “determine[d] as a matter of law” (citing, e.g., *Oswego*, 647 N.E.2d at 745)); *Grgat*, 135 N.E.3d at 850-51 (OCSPA affirmative misrepresentation claim requires allegation of misrepresentation that would mislead a reasonable consumer); Tex. Bus. & Com. Code § 17.50(a) (TDTPA affirmative misrepresentation claim requires detrimental reliance on the defendant’s material misrepresentation); *Deburro*, 2013 WL 5917665, at \*5 (same).

**C. Plaintiffs State No Bellwether Claim for “Unfair” Trade Practices.**

The FDUTPA, ICFA, and OCSA permit claims for “unfair” trade practices.<sup>29</sup> The Named Plaintiffs from Florida and Illinois fail to state such claims. There is no named Ohio plaintiff to assert such a claim under Ohio law.

The sound reasoning of *Hauck* is applicable to any unfairness claim under Florida or Illinois law. The Ninth Circuit reasoned that the plaintiffs’ unfairness claim there failed because they could not “plausibly allege[] that the harm represented by the theoretical risk of a cybersecurity flaw that has not yet been successfully exploited outweighs the other benefits of [the] processor design.” 2020 WL 2510754, at \*2. On that basis, the Ninth Circuit affirmed dismissal of a claim against AMD for “unfair” trade practices under the FDUTPA. Such a claim requires that the defendant’s conduct “offend[] established public policy” and be “immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers.” *PNR*, 842 So. 2d at 777 (citation omitted); *see Hauck*, 2020 WL 2510754, at \*2. This requires that the claimed injury “must not be outweighed by any countervailing benefits to consumers.” *See Porsche Cars N. Am., Inc. v. Diamond*, 140 So. 3d 1090, 1096-97 (Fla. Dist. Ct. App. 2014). The standard is the same in Illinois. *Batson v. Live Nation Entm’t, Inc.*, 746 F.3d 827, 830, 834 (7th Cir. 2014) (applying the same standard under the ICFA—an “unfair” practice must “offend[] public policy,” be “immoral, unethical, oppressive, or unscrupulous,” and/or “cause[] substantial injury to consumers” that is “not outweighed by any countervailing benefits”).<sup>30</sup> Allegations failing to

---

<sup>29</sup> The New Jersey, New York, and Texas Plaintiffs do not assert unfairness claims. *See* AC ¶¶ 1239-47, 1260-67, 1414-30.

<sup>30</sup> A plaintiff may not premise an “unfair” practices claim under the ICFA solely on deceptive practices (just as Judge Koh found, and the Ninth Circuit affirmed, is true for the UCL, *see supra* pp. 30-31). *Halperin v. Int’l Web Servs., LLC*, 123 F. Supp. 3d 999, 1007 (N.D. Ill. 2015).

meet this standard should be dismissed as a matter of law. *Hauck*, 2020 WL 2510754, at \*2; *Batson*, 746 F.3d 827 at 834-35. Here, as in *Hauck*, Plaintiffs cannot “plausibly allege[] that the harm represented by the theoretical risk of a cybersecurity flaw that has not yet been successfully exploited outweighs the other benefits of [Intel’s] processor design.” 2020 WL 2510754, at \*2. That is especially true where the alleged “defects”—i.e., Intel’s design choices—improved CPU performance, which Plaintiffs expressly admit is of critical importance to them. *See* AC ¶¶ 682-88. The FDUTPA and ICFA claims should be dismissed.

Finally, there is no Named Plaintiff to advance any “unfairness” claim under the OCSA, and any such claim fails for this reason. But even were there a named Ohio Plaintiff, there would be no viable unfairness claim under the OCSA. The OCSA count grounds Intel’s purported “unfair” conduct in the same statutory provision (Ohio Rev. Code § 1345.02(B)(1)-(2)) and the same actions (Intel’s alleged representations in connection with Ohio consumer transactions) as Intel’s purported “deceptive” conduct. *See* AC ¶ 1296. But Intel made no actionable misrepresentation, nor any actionable omission. The OCSA claim does not allege any other “unfair” conduct by Intel, and any unfairness claim therefore likewise fails.

#### **D. Plaintiffs State No Bellwether Claim for “Unconscionable” Conduct.**

The Florida, New Jersey, Ohio, and Texas statutes at issue permit claims for “unconscionable” practices.<sup>31</sup> The conduct here does not meet that standard by a long shot.

*First*, the Florida Plaintiff—Schwartz Eye—plainly fails to satisfy the standard for unconscionability under the FDUTPA, which requires an “absence of meaningful choice” together with “unreasonable[] . . . terms.” *Coffey v. WCW & Air, Inc.*, 2020 WL 3250744, at \*3

---

<sup>31</sup> The Illinois and New York Named Plaintiffs do not assert claims for unconscionable conduct. *See* AC ¶¶ 1009-19, 1260-67.

(N.D. Fla. Mar. 25, 2020) (citation omitted). Schwartz Eye does not allege—much less explain how—it lacked a “meaningful choice,” or that it faced terms that were “unreasonable.” *See id.* at \*3 (citation omitted). Instead, it simply lists “unconscionability” alongside its claims for unfair and deceptive practices. AC ¶ 960. Such a conclusory allegation is insufficient as a matter of law. *Iqbal*, 556 U.S. at 678-79. And in any event, where Schwartz Eye’s fraud and unfairness claims fail, so too should any claim of unconscionability. A plaintiff that cannot assert a claim for *unfair* practices under the FDUTPA also cannot state a claim for *unconscionable* practices under that statute. *See Rogers v. Cisco Sys., Inc.*, 268 F. Supp. 2d 1305, 1315 n.19 (N.D. Fla. 2003) (“[I]t is difficult to conceive of an ‘unconscionable’ act or practice that would not also be ‘unfair.’” (citation omitted)). The FDUTPA unconscionability claim should be dismissed.

*Second*, the New Jersey “courts . . . ‘have been careful to constrain [claims of unconscionable conduct under the NJCFA] to fraudulent, deceptive or other similar kind of selling or advertising practices.’” *Slebodnik v. Reynolds & Reynolds Co.*, 2014 WL 6609132, at \*5 (D.N.J. Nov. 20, 2014) (quoting *D’Agostino v. Maldonado*, 78 A.3d 527, 540 (N.J. 2013)); *see* N.J. Stat. Ann. § 56:8-2. Accordingly, the New Jersey Plaintiffs cannot state a claim for “unconscionable” conduct based on Intel’s design choices where they can show no fraudulent or deceptive conduct. This claim should be dismissed as a matter of law. *See Slebodnik*, 2014 WL 6609132, at \*8, \*10.

*Third*, the OCSA count alleges no “[u]nconscionable acts or practices.” Ohio Rev. Code § 1345.03. Such acts are those in which a supplier “manipulat[es] a consumer’s understanding.” *Johnson v. Microsoft Corp.*, 834 N.E.2d 791, 800 (Ohio 2005). A “focus” of such a claim is “on whether the consumer lacks the physical or mental ability to protect himself or herself.” *See Barrett-O’Neill v. Lalo, LLC*, 171 F. Supp. 3d 725, 741 (S.D. Ohio 2016)

(citation omitted); Ohio Rev. Code § 1345.03. With no Ohio purchaser identified at all, Plaintiffs plainly have alleged no unconscionable act. Regardless, the Complaint fails to allege that Intel—which *at most* had knowledge of *theoretical* vulnerabilities until the discovery of Spectre—“knowingly t[ook] advantage” of consumers, or “required” them to enter into a “substantially one-sided” transaction. AC ¶ 1297 (citing Ohio Rev. Code § 1345.03(B)(1), (5)). Consumers do not reasonably believe that their devices are “completely impervious to novel cybersecurity threats,” and there is nothing “unconscionable” about Intel implementing design features that enhanced performance in exchange for, *at most*, a “theoretical risk.” *See Hauck*, 2020 WL 2510754, at \*2.

*Fourth*, to plead an “unconscionable” practice under the TDTPA the plaintiff must allege conduct that “[took] advantage of the lack of knowledge, ability, experience, or capacity of the consumer to a grossly unfair degree.” Tex. Bus. & Com. Code §§ 17.45(5), 17.50(a)(3). “Gross” unfairness—i.e., “glaringly noticeable, flagrant, complete and unmitigated” unfairness—is an objective standard, and thus suitable for dismissal at the pleading stage. *Chastain v. Koonce*, 700 S.W.2d 579, 582-84 (Tex. 1985). Courts do not hesitate to dismiss such claims where the plaintiff’s allegation merely “parrots the statutory language.” *Jaramillo v. Liberty Mut. Ins. Co.*, 2019 WL 8223608, at \*7 (N.D. Tex. Apr. 29, 2019). That is precisely the case here. AC ¶ 1423. Because the Amended Complaint fails to state a claim for unfair practices, and the bar for unconscionability is higher than “mere unfairness,” the Named Plaintiff from Texas cannot state a claim for unconscionable practices. *See Chastain*, 700 S.W.2d at 582.

**E. No Bellwether Claim Can Advance Without a Named Plaintiff.**

No Named Plaintiff resides in Ohio or acquired an Intel CPU in Ohio, and therefore no plaintiff has standing to bring claims under Ohio consumer protection law.<sup>32</sup> *See Pardini v. Unilever U.S., Inc.*, 961 F. Supp. 2d 1048, 1061 (N.D. Cal. 2013). This Court already found that Plaintiffs may not “maintain a state subclass without a named representative from that state,” and that “[w]here . . . a representative plaintiff is lacking for a particular state, *all* claims based on that state’s laws are subject to dismissal.” MTD Order 61 (quoting *Pardini*, 961 F. Supp. 2d at 1061). As the Court noted, Plaintiffs cannot “bring a state-specific claim under [a state] consumer protection law” where Plaintiffs allege no transaction in that jurisdiction, and “there is thus no allegation from which th[at state’s] consumer protection law can arise.” *Id.*

**CONCLUSION**

For the foregoing reasons, all of the California-law claims and all of the state subclass counts identified above should be dismissed with prejudice.

---

<sup>32</sup> Plaintiffs dropped from the Amended Complaint a previously proposed Ohio subclass representative. ECF No. 115 ¶ 94.

DATED: July 28, 2020.

Respectfully submitted,

STOEL RIVES LLP

/s/ Steven T. Lovett

Steven T. Lovett, OSB No. 910701

steve.lovett@stoel.com

Rachel C. Lee, OSB No. 102944

rachel.lee@stoel.com

Telephone: 503.224.3380

WILLIAMS & CONNOLLY LLP

Daniel F. Katz (*pro hac vice*)

dkatz@wc.com

David S. Kurtzer-Ellenbogen (*pro hac vice*)

dkurtzer@wc.com

Telephone: 202.434.5000

Attorneys for Defendant Intel Corporation